Reactance Perturbation for Detecting and Identifying FDI Attacks in Power System State Estimation

Chensheng Liu, *Student Member, IEEE*, Jing Wu, *Member, IEEE*, Chengnian Long, *Member, IEEE*, and Deepa Kundur, *Fellow, IEEE*

***Abstract*—False data injection (FDI) attacks have recently been introduced as an important class of cyberattacks in modern power systems. By coordinating the injection of false data in selected meters readings, an FDI attacks can bypass bad data detection methods in power system state estimation. In this paper, we propose a strategy to enhance detection and identification of an FDI that leverages reactance perturbation. We begin by deriving conditions to mitigate attacks in noiseless systems that relates the likelihood of attack detection and identification to the rank of the composite matrix, limited by power system topology and the deployment of meters. Based on such conditions, we design a secure reactance perturbation algorithm that maximizes the likelihood of an FDI attack detection and identification while minimizing the effect on the operational cost of power systems, e.g., power losses on transmission lines. Simulations on a 6-bus and the IEEE 57-bus system verify the performance of the secure reactance perturbation and the effect on power losses in both noiseless and noisy systems.**

***Index Terms*—False data injection attacks, attack detection and identification, secure reactance perturbation.**

I. Introduction

CRITICAL infrastructure is undergoing a cyber-enablement whereby operational technology is being integrated with advanced computation and communication capabilities. This is especially evident in the modern power system [1] whereby this cyber-physical marriage promises to improve overall stability and efficiency, but at the cost of increased vulnerability to cyberattack [2]. For instance, it has been recently shown that an opponent may make use of authentication weaknesses and the *restart communications option* vulnerability in Modbus/TCP protocols, to inject false data into power grid meter readings [3].

Moreover, leveraging such power system vulnerabilities, attackers can coordinately "hack" the readings of multiple meters to stealthily mislead fundamental applications in power systems. For example, as an important class of cyberatacks against the integrity of telemetry measurements, false data injection (FDI) attacks can coordinate the injected false data in state estimation to stealthily mislead the results of state estimation [4]. In the context of power system state estimation, "stealthy" means that FDI attacks can bypass *measurement residual* based *bad data detection* methods by coordinating the injected false data based on information of *measurement matrix*, where measurement matrix is usually assumed to be fixed.

In this paper, we design an FDI mitigation approach that works by changing the effective state estimation measurement matrix such that attacks become more easily detectable and identifiable. Specifically, a power system reactance perturbation scheme is devised that aims to increase the probability of FDI detection and identification without introducing significant operational cost, e.g., power losses on transmission lines.

Existing strategies to design stealthy FDI attacks in state estimation that bypass bad data detection have been extensively studied in the literature. For example, to ensure the stealthy of FDI attacks, initial work on FDI attacks required that the injected bad data must be within the column space of the measurement matrix and assumed that the attacker had explicit knowledge of the measurement matrix [4]. Given that it is nontrivial for attackers to obtain the measurement matrix directly as its elements are related to the power system transmission lines' reactance values, related work focused on strategies to estimate the measurement matrix. Approaches using the transmission lines' parameter probability distribution and independent component analysis were proposed in [5] and [6], respectively; here secondary information such as probability distributions of power grid parameters are employed to relax the requirement of direct knowledge of the measurement matrix. Subsequently, in [7], a practical learning algorithm was proposed that did not require such secondary information. Instead, a basis of the measurement matrix was estimated from historical power system measurements. Thus, recent work suggests that stealthy FDI attacks are possible to achieve without explicit knowledge of the measurement matrix instead gleaning insights from operational information.

Manuscript received October 15, 2017; revised March 28, 2018; accepted June 6, 2018. Date of publication June 14, 2018; date of current version July 27, 2018. This work was supported in part by the National Nature Science Foundation under Grants 61673275 and 61473184 and in part by the China Scholarship Council. This paper was presented in part at the Fifth IEEE Global Conference on Signal and Information Processing (GlobalSIP), Montreal, QC, Canada, November 2017. The guest editor coordinating the review of this paper and approving it for publication was Dr. Javier Contreras. *(Corresponding authors: Jing Wu; Chengnian Long.)*

C. Liu, J. Wu, and C. Long are with the Department of Automation, Shanghai Jiao Tong University, and the Key Laboratory of System Control and Information Processing, Ministry of China, Shanghai 200240, China (e-mail: cs_l@sjtu.edu.cn; jingwu@sjtu.edu.cn; longcn@sjtu.edu.cn).

D. Kundur is with the Department of Electrical and Computer Engineering, University of Toronto, Toronto, ON M5S 1A1, Canada (e-mail: dkundur@ece.utoronto.ca).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/JSTSP.2018.2846542

To deter FDI attacks in state estimation, critical measurement protection strategies have been designed in [8] and [9], where FDI attacks can be detected if a *basic set* of power system meters are protected. This approach, however, has been deemed time-consuming and costly in terms of deploying security enforcements, such as encryption, on all critical meters. Moreover, legacy devices, with a limited computing and storage capacities, cannot support such security enforcements. Given that attackers must explicitly know (i.e., directly observe or estimate) the measurement matrix to construct a stealthy FDI attack, a moving target defense (MTD) strategy is designed in [10], where the set of measurements considered in state estimation and the admittances[1] of a set of lines are randomized to obfuscate critical information related to state estimation. To ensure the performance of the MTD strategy, a hidden MTD strategy was subsequently designed in [11] and [12], where the MTD strategy can not be discovered by attackers using measurement residual based methods. Even though the MTD strategy can prevent attackers from obtaining critical information related to measurement matrix, the assumption that transmission line's admittance changes at each state estimation is nontrivial.

Distinct from MTD, topology perturbation approaches have been recently designed to detect FDI attacks in [13] and [14] where the system is modeled as a sensitivity matrix. By comparing the actual measurement values with those estimated via the sensitivity matrix, FDI attacks can be detected. Limitations of the approach include that 1) As only the dependency between transmission line's reactance and measurements is considered in modeling the sensitivity matrix, the detection accuracy may be affected by uncontrolled fluctuations in power systems, such as load fluctuations; 2) Since the relationship between detection probability and reactance perturbation is not analyzed, optimality can not be ensured in reactance perturbation. In our work, we propose a method to not only detect FDI attacks, but also identify the injected bad data. To overcome limitation 1), we explore the information advantage that unobservable FDI attacks are within the column space of measurement matrix, where the accuracy of detecting and identifying FDI attacks is not affected by uncontrolled fluctuations. Moreover, the relationship between the probability of detecting and identifying FDI attacks and reactance perturbation is analyzed to maximize the detection and identification probability.

In this paper, we design a reactance perturbation-based scheme to detect and identify originally covert FDI attacks on power system state estimation that enhances the security of state estimation without significantly increasing the operational cost in power systems. Specifically,

- We derive FDI attack detection conditions under a noiseless setting that are practical to apply and that relate the probability of FDI detection to the rank of a composite matrix. Compared with our previous work [15], we further relax the requirements on power systems in detecting FDI attacks utilizing defender's information advantage on measurement matrices.
- We analyze identification conditions for overall and partial FDI attacks, and design a FDI attack identification method, which can enhance the identification of originally covert FDI attacks.
- We formulate a secure reactance perturbation optimization problem and propose an associate algorithm, where the probabilities of detecting and identifying FDI attacks is maximized without significantly increasing operational cost. Compared with our previous work [15], the performance of both FDI attack mitigation and operational cost is verified in a more practical way, where the attack detection and identification probabilities are simulated in both noiseless and noisy systems, and the operational cost is verified using the practical alternating current (AC) power flow model.

The remainder of this paper is organized as follows. In Section II, we present the models for state estimation, FDI attacks, secure reactance perturbation, and the dependencies between power losses and reactance perturbation. FDI attack detection and identification conditions in noiseless systems are analyzed in Section III. Secure reactance perturbation optimization and monitor design are presented in Section IV. Numerical simulations and conclusions are provided in Section V and VI, respectively.

II. System Model

This section introduces the FDI attack model under the condition of measurement matrix changes in power system state estimation. Secure reactance perturbation in distributed flexible alternating current transmission systems (D-FACTS) is discussed as a feasible approach to change the state estimation measurement matrix. To analyze the effects on operational cost, a linear sensitivities model is given, which models the dependencies between power losses on transmission lines and reactance perturbation.

A. Notation

In this paper, we denote the power system under consideration as $(\mathcal{N}, \mathcal{A})$, where $\mathcal{N}$ is the set of buses and $\mathcal{A}$ represents the set of transmission lines. Let $\mathcal{N}_{-r}$ be the set of buses at the exclusion of the reference bus. Boldface lower case letters (e.g., $\boldsymbol{\theta}, \mathbf{x}$) represent vectors whereby individual elements are represented with subscripts. For example, θ_i denotes the ith element of the vector $\boldsymbol{\theta}$. Similarly, x_{ij} is the reactance of transmission line, connecting bus i and j, in reactance vector $\mathbf{x}$. Boldface upper case letters (e.g., $\mathbf{H}$) denote matrices. We employ subscript "0" to distinguish previous and current variable values. For example, $\mathbf{H_0}$ is the previous measurement matrix while $\mathbf{H}$ is the current measurement matrix value in state estimation. Moreover, variables preceded by Δ denote a change in the associated variable. Notations with an underline and an overline are the minimum and maximum values of the corresponding variables, respectively. For example, $\underline{P}_i^g$ and $\overline{P}_i^g$ are the minimum and maximum generation output values for the generator at bus i. To better clarify the main variables used in this paper, nomenclature is summarized in Table I.

[1] Even though they call the MTD strategy as admittance perturbation, only transmission line's reactance are changed in [10].

TABLE I
SUMMARY OF NOMENCLATURE

Notation	Definition
$\mathbf{z_a}$	Compromised measurement vector.
$\mathbf{a}$	FDI attack vector.
$\mathbf{e}$	Gaussian measurement noise vector.
$\boldsymbol{\theta}$	Bus voltage phase angle of buses (excluding reference bus).
$\mathbf{H}$	DC measurement matrix in state estimation.
h_i	The ith column of matrix $\mathbf{H}$.
x_{ij}	Reactance of branch ij (connecting bus i and j).
r_{ij}	Resistance of branch ij (connecting bus i and j).
V_i	Voltage magnitude at bus i.
$\mathbf{D}$	Sensor deployment matrix in the decomposition of $\mathbf{H}$.
$\mathbf{x}$	Branch reactance vector.
$\mathbf{X}$	Diagonal branch reactance matrix.
$\mathbf{A}$	The (arc-to-node) incidence matrix.
$\mathbf{M}$	Composite matrix of $\mathbf{H_0}$ and $\mathbf{H}$; $\mathbf{M} = [\mathbf{H_0}\ \mathbf{H}]$.
$\boldsymbol{\Lambda}$	Input to the FDI attack monitor.
$\boldsymbol{\Psi}$	Output of the FDI attack monitor.
$r(\cdot)$	The matrix rank operator.
$C(\cdot)$	The column space of the associate argument matrix.
$N(\cdot)$	The null space of the associate argument matrix.
P_{loss}	Power losses on transmission lines.

B. Power System State Estimation

Power system state estimation refers to the procedure of estimating system state variables (consisting of bus voltage phase angles) from a set of redundant measurements obtained from various locations of the power system. Although the relationship between state variables and measurements is described by a nonlinear measurement function, undetectabe conditions in AC state estimation are too complex to be directly used in analysis. In order to facilitate the analysis, AC state estimation is usually linearized by replacing the nonlinear measurement function in AC state estimation with its Jacobian matrices at the current state [16]. As DC state estimation, a specially linearized model for the measurement equations, is widely used in analyzing the security of state estimation [17], [18], we use DC power flow model to analyze the detection and identification of FDI attacks with the assumption that the bus voltage magitude are all equal to 1.0 per unit [19].

Specifically, we consider the following well-known DC power flow model [19]:

$$\mathbf{z} = \mathbf{H} \cdot \boldsymbol{\theta} + \mathbf{e},$$

where $\mathbf{z} \in R^m$ is the measurement vector, m is the number of measurements, $\boldsymbol{\theta} \in R^{n-1}$ represents the bus voltage phase angle vector (state variables) with the voltage phase angle of the reference bus omitted as typical in DC state estimation [19], n is the number of buses, $\mathbf{H} \in R^{m\times(n-1)}$ is the *measurement matrix* that maps system states to measurement values, and $\mathbf{e} \in R^m$ is the measurement noise modeled as Gaussian with diagonal covariance matrix $\mathbf{W}$:

$$\mathbf{W} = \mathrm{diag}(\sigma_1^{-2}, \sigma_2^{-2}, \ldots, \sigma_m^{-2}),$$

where σ_i is the standard derivation of measurement noise at the ith meter ($1 \le i \le m$). Utilizing the weighted least-square criterion [19], system states can be estimated as:

$$\hat{\boldsymbol{\theta}} = (\mathbf{H}^T\mathbf{W}\mathbf{H})^{-1}\mathbf{H}^T\mathbf{W}\mathbf{z}.$$

To detect and identify bad measurements introduced by a variety of telemetry errors such as meter failure, *residual*-based bad data detection tests are commonly employed within power system state estimation whereby the *measurement residual* $\mathbf{z} - \mathbf{H}\hat{\boldsymbol{\theta}}$ is given by the difference between the observed and estimated measurements. Specifically, for bad data detection using the χ^2-test, which is widely used in power system state estimation, bad data is detected when $\|\mathbf{z} - \mathbf{H}\cdot\hat{\boldsymbol{\theta}}\|^2 > \gamma^2$, where γ is a preset threshold related to the detection confidence probability (e.g., 95%).

C. FDI Attacks Under Measurement Matrix Changes

As formulated in the foundational paper by Liu *et al.* [4], an FDI attack on state estimation can be modeled as:

$$\mathbf{z_a} = \mathbf{z} + \mathbf{a} = \mathbf{H}\cdot\boldsymbol{\theta} + \mathbf{a} + \mathbf{e}, \tag{1}$$

where $\mathbf{z_a} \in R^m$ is the compromised measurement vector and $\mathbf{a} \in R^m$ is the attack vector representing falsely injected values into the legitimate measurement values $\mathbf{z} \in R^m$.

Even though attack vector $\mathbf{a} \in R^m$ can be any value, e.g., replay attacks [20] and scaling attacks [21], the injected data $\mathbf{a}$ need to be well cordinated to bypass bad data detection in state estimation. For example, to avoid being detected by residual-based bad data detection, FDI attacks must satisfy $\mathbf{a} = \mathbf{H}\cdot\Delta\boldsymbol{\theta}$, which has been shown to be equivalent to $\mathbf{a} \in C(\mathbf{H})$ [4]. This ensures that the measurement residual under attack is consistent with the residual under normal (legitimate) conditions:

$$\begin{aligned}\|\mathbf{z_a} - \mathbf{H}\cdot\hat{\boldsymbol{\theta}}_{\mathbf{bad}}\| &= \|\mathbf{z} + \mathbf{a} - \mathbf{H}(\hat{\boldsymbol{\theta}} + \Delta\boldsymbol{\theta})\| \\ &= \|\mathbf{z} - \mathbf{H}\cdot\hat{\boldsymbol{\theta}} + (\mathbf{a} - \mathbf{H}\cdot\Delta\boldsymbol{\theta})\| \\ &= \|\mathbf{z} - \mathbf{H}\cdot\hat{\boldsymbol{\theta}}\| < \gamma,\end{aligned}$$

where $\Delta\boldsymbol{\theta}$ are the changes in state variable estimates introduced by attack vector $\mathbf{a}$. Even though attackers can also bypass bad data detection by exploring the information of measurement noise, the changes in states introduced by such attacks are small and such method cannot ensure the stealth of attacks. It means that attack vector $\mathbf{a} \notin C(\mathbf{H})$ is very likely to be detected. Hence, in this paper, we focus on unobservable FDI attacks satisfying $\mathbf{a} \in C(\mathbf{H})$, which does great damage to state estimation.

Note from the above discussion that the FDI attacker must exactly know the measurement matrix $\mathbf{H}$ to successfully evade bad data detection in state estimation. Even though it appears nontrivial to exactly know $\mathbf{H}$ [10] ($\mathbf{H}$ is a function of branch reactance only [19]), it has been shown that attackers can estimate a basis of column space $C(\mathbf{H})$, $\hat{\mathbf{H}}$, from a large volume of historical measurements using a subspace estimation algorithm [7]. The reader should note that since $r(\mathbf{H}) = r(\hat{\mathbf{H}}) = n - 1$, $\mathbf{H} \in R^{m\times(n-1)}$, $\hat{\mathbf{H}} \in R^{m\times(n-1)}$, $\mathbf{H}$ and $\hat{\mathbf{H}}$ are both a basis of $C(\mathbf{H})$. Therefore, for any attack vector $\mathbf{a} = \hat{\mathbf{H}}\cdot\Delta\boldsymbol{\theta}'$, there exists $\Delta\boldsymbol{\theta}$, such that $\mathbf{a} = \hat{\mathbf{H}}\cdot\Delta\boldsymbol{\theta}' = \mathbf{H}\cdot\Delta\boldsymbol{\theta}$, and the injected attack vector can be expressed as $\mathbf{a} = \mathbf{H}\cdot\Delta\boldsymbol{\theta}$, equivalently. Hence, the attacker can compute an unobservable FDI attack vector $\mathbf{a}$ from historical measurements without explicit knowledge of $\mathbf{H}$.

We now consider the case in which the measurement matrix changes. Suppose the measurement matrix is estimated from historical measurements related to a previous measurement matrix $\mathbf{H}_0$, which differs from the current new measurement matrix $\mathbf{H}$. The injected attack vector then satisfies $\mathbf{a} = \mathbf{H}_0 \cdot \Delta\boldsymbol{\theta}$, i.e., $\mathbf{a} \in C(\mathbf{H}_0)$. The effect of a change in measurement matrix from $\mathbf{H}_0$ to $\mathbf{H}$, can be expressed as:

$$\mathbf{z_a} = \mathbf{H} \cdot \boldsymbol{\theta} + \mathbf{H}_0 \cdot \Delta\boldsymbol{\theta} + \mathbf{e}, \tag{2}$$

where $\mathbf{H}_0$ is the previous measurement matrix known to the attacker, $\mathbf{H}$ is the current measurement matrix unknown to the attacker, and the system operator knows that $\mathbf{a} \in C(\mathbf{H}_0)$. We return to the model of (2) in Section III where we discuss how changes in the measurement matrix enable improved FDI attack detection and identification.

D. Secure Reactance Perturbation in D-FACTS

Given that the measurement matrix $\mathbf{H}$ is a function of branch reactance alone, we assert in this paper that *reactance perturbation* is a feasible approach to deliberately modify the measurement matrix $\mathbf{H}$ used in state estimation to aid in FDI attack mitigation; we call this *secure reactance perturbation*. By connecting directly to transmission lines, D-FACTS devices, such as distributed static series compensators (DSSCs), are capable of changing line impedance dynamically [22]. We contend that for secure reactance perturbation, the changes in reactance are limited by the following constraints:

1) The reactance changes are limited by the capacities of D-FACTS devices, i.e.,

$$\underline{\tau} \cdot \mathbf{x}_0 \leq \Delta\mathbf{x} \leq \overline{\tau} \cdot \mathbf{x}_0, \tag{3}$$

where $\mathbf{x}_0$ is the actual reactance vector under rated current conditions that consists of all branch reactance values for each transmission line, $\Delta\mathbf{x} \in R^p$ represents the change in branch reactance vector and p is the number of branches in power system. Limits $\underline{\tau} \cdot \mathbf{x}_0$ and $\overline{\tau} \cdot \mathbf{x}_0$ denote the minimum and maximum possible change to the reactance vector. For example, the reactance changes of DSSC is up to $\pm 10 \sim 20\%$ of the actual line reactance under rated current conditions [23].

2) If there is a reactance change in a transmission line, the change cannot be so small that there is negligible impact on enhancing attack detection and identification [10]. Hence, the reactance change must satisfy:

$$\Delta x_{ij} = 0 \text{ or } |\Delta x_{ij}| \geq \omega \cdot |x_{0ij}|, \ \ ij \in \mathcal{A}, \tag{4}$$

where x_{0ij} is the reactance of branch ij in vector $\mathbf{x}_0$ and ω is the ratio of the minimum magnitude change in reactance over the line reactance magnitude.

E. Power Losses Dependencies on Reactance Perturbation

To obtain the impact of secure reactance perturbation on the operational cost in power systems, we use AC power flow model, such as AC optimal power flow (AC-OPF) in analysis, where the changes in operational cost introduced by reactance perturbation can be modeled accurately. However, it is difficult to calculating the Jacobian of the vector function [26] in solving the modified AC-OPF, where line reactances are also considered as variables. Instead, the impact on the operational cost can be quantified, in part, by the transmission line real power losses, which can be expressed as a summation of the real power losses on all lines. Linear sensitivities are used in this paper to formulate the dependencies between power losses and reactance perturbation, which is widely used to explain how quantities of interest concering lines, buses and flows in power systems are affected by a slight change of another quantity somewhere else [24].

For the given power systems $(\mathcal{N}, \mathcal{A})$, the total real power losses are

$$P_{loss} = \sum_{ij \in \mathcal{A}} |I_{ij}| \cdot r_{ij}, \tag{5}$$

where the power loss on a line can be expressed in terms of the current magnitude and line resistance [24], and the line current flow magnitude from bus i to bus j can be expressed as [19]

$$I_{ij} = \sqrt{(g_{ij}^2 + b_{ij}^2)(V_i^2 + V_j^2 - 2V_i \cdot V_j \cdot \cos\theta_{ij})}. \tag{6}$$

Note that $g_{ij} + j \cdot b_{ij}$ is the admittance of the series branch connecting buses i and j, i.e.,

$$g_{ij}^2 + j \cdot b_{ij}^2 = \frac{r_{ij}}{r_{ij}^2 + x_{ij}^2} + j \cdot \frac{-x_{ij}}{r_{ij}^2 + x_{ij}^2}. \tag{7}$$

The dependencies between power losses and line reactance can be derived from (5). For a given transmission line connecting bus i and j, it can be calculated by solving the following partial differential:

$$\frac{dP_{loss}}{dx_{ij}} = \frac{\partial P_{loss}}{\partial s_{(\theta,V)}} \cdot \frac{\partial s_{(\theta,V)}}{\partial x_{ij}} + \frac{\partial P_{loss}}{\partial g_{ij}} \cdot \frac{\partial g_{ij}}{\partial x_{ij}} + \frac{\partial P_{loss}}{\partial b_{ij}} \cdot \frac{\partial b_{ij}}{\partial x_{ij}}, \tag{8}$$

where the vector $s_{(\theta,V)}$ is a concatenated vector of all the angle and voltage states for the system. In (8), $\frac{\partial s_{(\theta,V)}}{\partial x_{ij}}$ can be calculated using methods in [24], and the other parts can be calculated directly.

Suppose the current line reactance vector is $\mathbf{x}$, the changes in line reactance is $\Delta\mathbf{x}$, and the new line reactance is $\mathbf{x}_0 + \Delta\mathbf{x}$. The best linear approximation to the power losses with a line reactance $\mathbf{x} + \Delta\mathbf{x}$ can be expressed as

$$P_{loss}(\mathbf{x} + \Delta\mathbf{x}) \approx P_{loss}(\mathbf{x}) + LS(\mathbf{x}) \cdot \Delta\mathbf{x}, \tag{9}$$

where $P_{loss}(\mathbf{x})$ is the power losses with a line reactance $\mathbf{x}$, and $LS(\mathbf{x})$ is the linear sensitivities matrix with a line reactance $\mathbf{x}$, and $LS(\mathbf{x}) \cdot \Delta\mathbf{x}$ is the approximate changes in power losses introduced by line reactance perturbation.

III. Attack Detection and Identification for Secure Reactance Perturbation

Similar to the observability analysis in control systems [25], in this section, we analyze FDI attack detection and identification conditions for secure reactance perturbation under a noiseless setting. Overall conditions for detecting and identifying all possible FDI attacks are first developed. Given the high degree of constraints imposed on power system topology and the deployment of meters by these general conditions, requirements for detecting and identifying partial FDI attacks are then analyzed to represent more feasible protection scenarios.

A. General Detection and Identification Conditions

From (2), we model FDI attacks in the presence of secure reactance perturbation under a noiseless setting as follows:

$$\mathbf{z_a} = \mathbf{H} \cdot \boldsymbol{\theta} + \mathbf{H}_0 \cdot \Delta\boldsymbol{\theta}, \tag{10}$$

where the measurement matrix known to attackers is given by $\mathbf{H}_0$, and the real measurement matrix is $\mathbf{H}$. Similar to [27], we assume the presence of an attack *monitor* in power system state estimation with input $\boldsymbol{\Lambda} = \{\mathbf{H}_0, \mathbf{H}, \mathbf{z_a}\}$ and output $\boldsymbol{\Psi}(\boldsymbol{\Lambda}) = \{\psi_1(\boldsymbol{\Lambda}), \psi_2(\boldsymbol{\Lambda})\}$, where the detection output $\psi_1(\boldsymbol{\Lambda}) \in \{\text{True}, \text{False}\}$ (in relation to the presence of an FDI attack), and the estimated attack vector $\psi_2(\boldsymbol{\Lambda}) \in R^m$.

Attack detection and identification in reactance perturbation can be defined as follows:

Definition 1 (*Attack Detection and Identification*): Consider the scenario of (10) with a nonzero FDI attack $\mathbf{a} = \mathbf{H}_0 \cdot \Delta\boldsymbol{\theta}$, and the presence of a monitor with input $\boldsymbol{\Lambda} = \{\mathbf{H}_0, \mathbf{H}, \mathbf{z_a}\}$ and output $\boldsymbol{\Psi}(\boldsymbol{\Lambda}) = \{\psi_1(\boldsymbol{\Lambda}), \psi_2(\boldsymbol{\Lambda})\}$. The FDI attack $\mathbf{a}$ is *detected* by the monitor if $\psi_1(\boldsymbol{\Lambda}) = \text{True}$. The FDI attack $\mathbf{a}$ is *identified* by the monitor if $\psi_2(\boldsymbol{\Lambda}) = \mathbf{a}$.

The definition above is similar to that of [27]. The distinction lies in the fact that Definition 1 requires the identification of the particular attack vector (i.e., $\psi_2(\boldsymbol{\Lambda}) = \mathbf{a}$) while the monitor in [27] only detects the non-zero elements of $\mathbf{a}$ representing the set of attacked meters without knowledge of the particular injected values.

Similar to Lemma 3.1 in [27], undetectable FDI attacks in reactance perturbation are expressed as follows:

Lemma 1 (Undetectable Attack in Reactance Perturbation): Any attack vector $\mathbf{a} = \mathbf{H}_0 \cdot \Delta\boldsymbol{\theta}$, $\Delta\boldsymbol{\theta} \in R^{n-1}$, $\Delta\boldsymbol{\theta} \neq \mathbf{0}$, is undetectable with new measurement matrix $\mathbf{H}$ in reactance perturbation if and only if there exist $\boldsymbol{\theta}$ and $\boldsymbol{\theta}'$ such that $\mathbf{H} \cdot \boldsymbol{\theta} + \mathbf{H}_0 \cdot \Delta\boldsymbol{\theta} = \mathbf{H} \cdot \boldsymbol{\theta}'$.

Similarly, unidentifiable FDI attacks in reactance perturbation can be expressed as follows:

Lemma 2 (Unidentifiable Attack in Reactance Perturbation): Any attack vector $\mathbf{a} = \mathbf{H}_0 \cdot \Delta\boldsymbol{\theta}, \Delta\boldsymbol{\theta} \in R^{n-1}, \Delta\boldsymbol{\theta} \neq \mathbf{0}$, is unidentifiable if and only if there exist $\boldsymbol{\theta}, \boldsymbol{\theta}'$ and $\Delta\boldsymbol{\theta}', \Delta\boldsymbol{\theta}' \neq \Delta\boldsymbol{\theta}$, such that $\mathbf{H} \cdot \boldsymbol{\theta} + \mathbf{H}_0 \cdot \Delta\boldsymbol{\theta} = \mathbf{H} \cdot \boldsymbol{\theta}' + \mathbf{H}_0 \cdot \Delta\boldsymbol{\theta}'$.

It is clear that an undetectable attack is a special case of an unidentifiable attack in reactance perturbation, i.e., when $\Delta\boldsymbol{\theta}' = 0$. This implies that an undetectable attack must be an unidentifiable attack, and, inversely, an identifiable attack must be a detectable attack.

Lemma 1 and 2 give undetectable and unidentifiable conditions for FDI attacks in reactance perturbation, respectively. General condition for detecting and identifying all the possible FDI attacks in reactance perturbation can be expressed as follows; we employ the term *originally covert attack* to refer to the stealth of the attack prior to reactance perturbation.

Remark 1 (General Detection Condition): The originally covert attack $\mathbf{a} = \mathbf{H}_0 \cdot \Delta\boldsymbol{\theta}, \Delta\boldsymbol{\theta} \in R^{n-1}, \Delta\boldsymbol{\theta} \neq \mathbf{0}$, is detectable if and only if for any $\boldsymbol{\theta}$ and $\boldsymbol{\theta}'$, $\mathbf{H} \cdot (\boldsymbol{\theta}' - \boldsymbol{\theta}) \neq \mathbf{H}_0 \cdot \Delta\boldsymbol{\theta}$ holds.

Remark 2 (General Identification Condition): The originally covert attack $\mathbf{a} = \mathbf{H}_0 \cdot \Delta\boldsymbol{\theta}$, $\Delta\boldsymbol{\theta} \in R^{n-1}$, $\Delta\boldsymbol{\theta} \neq \mathbf{0}$, is identifiable if and only if for any $\boldsymbol{\theta}, \boldsymbol{\theta}'$ and $\Delta\boldsymbol{\theta}'$, $\Delta\boldsymbol{\theta} \neq \Delta\boldsymbol{\theta}'$, $\mathbf{H} \cdot (\boldsymbol{\theta}' - \boldsymbol{\theta}) \neq \mathbf{H}_0 \cdot (\Delta\boldsymbol{\theta} - \Delta\boldsymbol{\theta}')$ holds.

Even though Remark 1 and 2 give sufficient and necessary conditions for detecting and identifying FDI attacks in reactance perturbation, such conditions can hardly be used for calculation. An equivalent detection and identification condition is presented below:

Theorem 1 (Equivalent Detection and Identification Condition): The originally covert attack $\mathbf{a} = \mathbf{H}_0 \cdot \Delta\boldsymbol{\theta}, \Delta\boldsymbol{\theta} \in R^{n-1}$, $\Delta\boldsymbol{\theta} \neq \mathbf{0}$, is detectable and identifiable in reactance perturbation with a new measurement matrix $\mathbf{H}$ if and only if $r(\mathbf{M}) = 2 \cdot (n-1)$, where $\mathbf{M} = [\mathbf{H}_0\ \mathbf{H}], \mathbf{H}_0, \mathbf{H} \in R^{m \times (n-1)}$.

Proof: First, we prove the equivalent detection condition for FDI attacks.

(If): Suppose the originally covert attack $\mathbf{a} = \mathbf{H}_0 \cdot \Delta\boldsymbol{\theta}, \Delta\boldsymbol{\theta} \in R^{n-1}, \Delta\boldsymbol{\theta} \neq \mathbf{0}$ is detectable in reactance perturbation, we have $\mathbf{H} \cdot (\boldsymbol{\theta}' - \boldsymbol{\theta}) \neq \mathbf{H}_0 \cdot \Delta\boldsymbol{\theta}$ holds for any $\boldsymbol{\theta}, \boldsymbol{\theta}'$ and $\Delta\boldsymbol{\theta} \neq \mathbf{0}$. This means that for any $\Delta\boldsymbol{\theta} \neq \mathbf{0}$,

$$\begin{bmatrix}\mathbf{H}_0\ \mathbf{H}\end{bmatrix} \cdot \begin{bmatrix}\Delta\boldsymbol{\theta} \\ \boldsymbol{\theta} - \boldsymbol{\theta}'\end{bmatrix} \neq \mathbf{0}. \tag{11}$$

Therefore, for any $\Delta\boldsymbol{\theta} \neq \mathbf{0}$ there is no vector $[\Delta\boldsymbol{\theta}^T\ (\boldsymbol{\theta} - \boldsymbol{\theta}')^T]^T$ in null space $N(\mathbf{M})$. Since $r(\mathbf{H}) = n-1$, we have $\mathbf{H} \cdot (\boldsymbol{\theta}' - \boldsymbol{\theta}) \neq \mathbf{0}$ when $\Delta\boldsymbol{\theta} = \mathbf{0}$ and $\boldsymbol{\theta} - \boldsymbol{\theta}' \neq \mathbf{0}$. That is, (11) holds and such vectors are not in $N(\mathbf{M})$, either. We have $N(\mathbf{M}) = \{\mathbf{0}\}$, i.e., $r(\mathbf{M}) = 2 \cdot (n-1)$.

(Only if): Suppose $r(\mathbf{M}) = 2 \cdot (n-1)$, we have $N(\mathbf{M}) = \{\mathbf{0}\}$. This means that for any $\Delta\boldsymbol{\theta} \neq \mathbf{0}$, (11) holds. Then for any $\boldsymbol{\theta}, \boldsymbol{\theta}', \Delta\boldsymbol{\theta} \in R^{n-1}$, $\Delta\boldsymbol{\theta} \neq \mathbf{0}$, $\mathbf{H} \cdot (\boldsymbol{\theta}' - \boldsymbol{\theta}) \neq \mathbf{H}_0 \cdot \Delta\boldsymbol{\theta}$ holds, and any attack vector $\mathbf{a} = \mathbf{H}_0 \cdot \Delta\boldsymbol{\theta}$, $\Delta\boldsymbol{\theta} \neq \mathbf{0}$, is detectable.

The proof of the equivalent identification condition is similar to the proof above. ■

Theorem 1 can be further explained with state estimation theory. Reformulating (10) in matrix form gives:

$$\mathbf{z_a} = \begin{bmatrix}\mathbf{H}_0\ \mathbf{H}\end{bmatrix} \cdot \begin{bmatrix}\Delta\boldsymbol{\theta} \\ \boldsymbol{\theta}\end{bmatrix}, \tag{12}$$

$[\Delta\boldsymbol{\theta}^T\ \boldsymbol{\theta}^T]^T$ can be estimated accurately when system states are observable, i.e., $r(\mathbf{M}) = 2 \cdot (n-1)$. This implies that the attack vector $\mathbf{a} = \mathbf{H}_0 \cdot \Delta\boldsymbol{\theta}$ can be identified when $r(\mathbf{M}) = 2 \cdot (n-1)$. As identifiable attacks are also detectable, any attack vector $\mathbf{a} = \mathbf{H}_0 \cdot \Delta\boldsymbol{\theta}$ is detectable when $r(\mathbf{M}) = 2 \cdot (n-1)$.

Even though any FDI attack can be detected and identified if the *composite matrix* $\mathbf{M} = [\mathbf{H}_0\ \mathbf{H}]$ is full column rank, i.e., $r(\mathbf{M}) = 2 \cdot (n-1)$, we assert that such a condition may be too restrictive to apply to many power systems in practice. In the next section, we explore the constraints on power system topology and meters introduced by the equivalent detection and identification conditions in Theorem 1.

B. Limits on Topology and Meters in General Conditions

In order to analyze the limits on power systems topology and meters in Theorem 1, we describe the power system

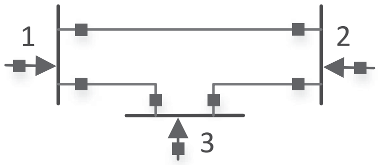


Fig. 1. A fully measured 3-bus power system.

topology as an (arc-to-node) incidence matrix $\mathbf{A} \in R^{n\times p}$. For any transmission line $\ell = 1, \ldots, p$,

$$\mathbf{A}(i,\ell) = \begin{cases} 1 & \text{if branch } \ell \text{ starts at node } i \\ -1 & \text{if branch } \ell \text{ ends at node } i \\ 0 & \text{otherwise,} \end{cases}$$

where $p = |\mathcal{A}|$ is the number of transmission lines, -1 denotes that the direction of the flow is opposite to the direction of the arc.

According to [29], any measurement matrix in the DC state estimation can be decomposed into three parts:

$$\mathbf{H} = \mathbf{D} \cdot \mathbf{X} \cdot \mathbf{A}_{-r}^{T}, \tag{13}$$

where $\mathbf{D} \in R^{m\times p}$ is a meter deployment matrix, m is the number of meters, $\mathbf{X} \in R^{p\times p}$ is a diagonal reactance matrix, $\mathbf{A}_{-r} \in R^{(n-1)\times p}$ is a sub-matrix of $\mathbf{A}$, including all rows in $\mathbf{A}$ except the row corresponding to the reference bus. Note that the diagonal elements in matrix $\mathbf{X}$ are the reciprocal of the branch reactance, e.g., $1/x_{ij}$.

In fully measured power systems, there are meters of 1) power flow on transmission lines, 2) their negative copies, and 3) external power injections into nodes, in $2 \cdot p + n$ meters. As power flow can be linearly expressed as $\mathbf{X} \cdot \mathbf{A}_{-r}^{T} \cdot \boldsymbol{\theta}$, and the external power injections into nodes can also be formulated as $\mathbf{A} \cdot \mathbf{X} \cdot \mathbf{A}_{-r}^{T} \cdot \boldsymbol{\theta}$ [29], the meter deployment matrix $\mathbf{D}$ in fully measured power systems can be expressed as

$$\mathbf{D} = \begin{bmatrix} \mathbf{I} \\ -\mathbf{I} \\ \mathbf{A} \end{bmatrix}, \tag{14}$$

where $\mathbf{I} \in R^{p\times p}$ is an identity matrix.

As most of power systems are not fully measured, we use meter selection matrix $\mathbf{C}$ to choose the deployed meters from all the possible meters, where the entries in matrix $\mathbf{C}$ are 0 or 1. Note that only one entry is 1 in each row of matrix $\mathbf{C}$, and $C(i,j) = 1$ denotes that the jth meter of the $2 \cdot p + n$ meters (in fully measured power sysem) is measured. Hence, the measurement matrix $\mathbf{H}$ in (10) can be expressed as

$$\mathbf{H} = \mathbf{D} \cdot \mathbf{X} \cdot \mathbf{A}_{-r}^{T} = \mathbf{C} \cdot \begin{bmatrix} \mathbf{I} \\ -\mathbf{I} \\ \mathbf{A} \end{bmatrix} \cdot \mathbf{X} \cdot \mathbf{A}_{-r}^{T}, \tag{15}$$

where $\mathbf{C} \in R^{m\times(2\cdot p+n)}$ is an identify matrix in fully measured power systems.

As a simple case study, consider a fully measured 3-bus system [19] (Bus 3 is the reference bus) as shown in Fig. 1. The decomposition of the measurement matrix $\mathbf{H}$ can be expressed as:

$$\mathbf{H} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ \vdots & \vdots & \vdots \\ 1 & 1 & 0 \\ -1 & 0 & 1 \\ 0 & -1 & -1 \end{bmatrix} \cdot \begin{bmatrix} \frac{1}{x_{12}} & & \\ & \frac{1}{x_{13}} & \\ & & \frac{1}{x_{23}} \end{bmatrix} \cdot \begin{bmatrix} 1 & -1 \\ 1 & 0 \\ 0 & 1 \end{bmatrix},$$

where the first three lines of the left-most matrix are related to the meters on the 3 transmission lines, the last three lines are related to the external power injection at the 3 buses, and the middle three rows correspond to the negative copy of power flow on transmission lines. When the 3-bus power system is not fully measured, e.g., only external power injections are measured, the selection matrix $\mathbf{C}$ in (15) can be expressed as

$$\mathbf{C} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix},$$

where $C(1,7) = C(2,8) = C(3,9) = 1$ denotes external power injection are measured.

Using the decomposition above, the composite matrix $\mathbf{M}$ can be expressed as a function of the diagonal reactance matrix $\mathbf{X}$, explicitly:

$$\mathbf{M} = \begin{bmatrix} \mathbf{H}_0 \ \mathbf{H} \end{bmatrix} = \mathbf{D} \cdot \begin{bmatrix} \mathbf{X}_0 \ \mathbf{X} \end{bmatrix} \cdot \begin{bmatrix} \mathbf{A}_{-r}^{T} & \mathbf{0} \\ \mathbf{0} & \mathbf{A}_{-r}^{T} \end{bmatrix}, \tag{16}$$

where $\mathbf{X} = \text{diag}(\mathbf{x})$, $\mathbf{D}$ and $\mathbf{A}$ are not related to transmission lines' reactance.

To ensure the detection and identification of all the possible FDI attacks $\mathbf{a} = \mathbf{H}_0 \cdot \Delta\boldsymbol{\theta}$, the composite matrix must satisfy $r(\mathbf{M}) = 2 \cdot (n-1)$, according to Theorem 1. Utilizing the properties of matrices product, we have:

$$2 \cdot (n-1) \le \min \left\{ r(\mathbf{D}), r(\begin{bmatrix} \mathbf{X}_0 & \mathbf{X} \end{bmatrix}), r\left(\begin{bmatrix} \mathbf{A}_{-r}^{T} & \mathbf{0} \\ \mathbf{0} & \mathbf{A}_{-r}^{T} \end{bmatrix} \right) \right\}. \tag{17}$$

As for each line connecting bus i and j, $1/x_{ij} \neq 0$, we have $r(\mathbf{X}) = p$. Moreover, since $r(\mathbf{H}) = n-1$, $r(\mathbf{A}_{-r}) = n-1$ holds. Hence, (17) can be expressed as:

$$2 \cdot (n-1) \le \min\{r(\mathbf{D}),\ p,\ 2 \cdot (n-1)\}, \tag{18}$$

i.e., $p \ge 2 \cdot (n-1)$ and $r(\mathbf{D}) \ge 2 \cdot (n-1)$. Obviously, $p \ge 2 \cdot (n-1)$ suggests that the number of transmission lines must be no less than twice of the number of states, which represents a topology limitation. As $\mathbf{D} \in R^{m\times p}$, $r(\mathbf{D}) \ge 2 \cdot (n-1)$ denotes that not only the number of meters must be no less than twice of the number of states, but also the rank of meter deployment matrix $\mathbf{D}$ must be no less than twice of the number of states, which represents the limits on meters.

Even though the limits on topology and meters are only necessary conditions for the full column rank condition in Theorem 1, it is too restrictive to apply to some power systems. For example, in the fully measured 3-bus system as shown in Fig. 1, there are 2 states and 3 transmission lines, i.e., $n-1 = 2$

and $p = 3$. According to (18), we have

$$r(\mathbf{M}) \leq \min\{3, 3, 4\}.$$

That is, $r(\mathbf{M}) \leq 3$, i.e., the rank of the composite matrix in the 3-bus system is no larger than 3. Thus the composite matrix in the 3-bus systems is not full column rank, and it cannot detect and identify all possible FDI attacks.

In this section, we give the general detection and identification conditions for overall FDI attacks. In the next section, we analyze the detection and identification of FDI attacks in non-full column rank cases and derive attack detection and identification conditions for *partial* FDI attacks. This allows our results to be applicable to a broader class of power systems.

C. Partial Detection and Identification Conditions

We demonstrate in this section that partial FDI attacks can be detected through secure reactance perturbation even though the composite matrix $\mathbf{M}$ is not full column rank. We deduce the detection and identification conditions for partial FDI attacks based on the independence of columns in the composite matrix $\mathbf{M}$.

Theorem 2 (Partial Attack Detection Condition): For a given composite matrix $[\mathbf{H}_0\ \mathbf{H}]$, $\mathbf{H}_0, \mathbf{H} \in R^{m\times(n-1)}$, denote S^d as the index set of the columns in $\mathbf{H}_0$ excluding those linearly dependent on the columns of $\mathbf{H}$. Let $\mathbf{H}_0^d$ be the matrix consisting of columns in $\mathbf{H}_0$ indexed by S^d and $|S^d|$ be the cardinality of set S^d. Specific FDI attacks $\mathbf{a} = \mathbf{H}_0 \cdot \Delta\boldsymbol{\theta}$, $\Delta\boldsymbol{\theta} \in R^{n-1}$, where $\Delta\theta_i \neq 0$, and $i \in S^d$, can be detected if $r([\mathbf{H}_0^d\ \mathbf{H}]) = n - 1 + |S^d|$.

Proof: Denote $h_{0,i}$ and h_j as the ith column of $\mathbf{H}_0$ and the jth column of $\mathbf{H}$, respectively. Let $\mathcal{N}_{-r}$ be the index set of columns in $\mathbf{H}$ ($\mathcal{N}$ is the index set of all the buses and $\mathcal{N}_{-r}$ is the index set of buses except the reference bus). As $r([\mathbf{H}_0^d\ \mathbf{H}]) = n - 1 + |S^d|$, i.e., columns in $[\mathbf{H}_0^d\ \mathbf{H}]$ are linearly independent, for any $\Delta\theta_i \neq 0$, $i \in S^d$, and $\boldsymbol{\theta} \in R^{n-1}$, we have $\sum_{i\in S^d} \Delta\theta_i \cdot h_{0,i} \neq \sum_{j\in\mathcal{N}_{-r}} \theta_j \cdot h_j$. As $h_{0,i}$, $i \notin S^d$, is linearly dependent on columns of $\mathbf{H}$, for any $\Delta\theta_i$, there exist $\boldsymbol{\theta}' \in R^{n-1}$ such that $\sum_{i\notin S^d} \Delta\theta_i \cdot h_{0,i} = \sum_{j\in\mathcal{N}_{-r}} \theta'_j \cdot h_j$. For any FDI attacks $\mathbf{a} = \mathbf{H}_0 \cdot \Delta\boldsymbol{\theta}$, where $\Delta\theta_i \neq 0$, $i \in S^d$, we have $\mathbf{a} - \sum_{i\notin S^d} \Delta\theta_i \cdot h_{0,i} \neq \sum_{j\in\mathcal{N}_{-r}} \theta_j \cdot h_j$. This means that for any FDI attacks $\mathbf{a} = \mathbf{H}_0 \cdot \Delta\boldsymbol{\theta}$, where $\Delta\theta_i \neq 0$, $i \in S^d$, $\mathbf{a} \neq \sum_{j\in\mathcal{N}_{-r}} (\theta_j + \theta'_j) \cdot h_j$. That is, the specific FDI attacks are not in the column space of $\mathbf{H}$, and can be detected. ■

To demonstrate Theorem 2, we analyze the detection of FDI attacks in the 3-bus system shown in Fig. 1, where the reactance of the transmission lines are $x_{12} = 0.03$ p.u., $x_{13} = 0.05$ p.u. and $x_{23} = 0.08$ p.u. The rank of the composite matrix increases from 2 to 3 by updating the reactance of transmission line, connecting bus 1 and 2, from 0.03 p.u. to 0.033 p.u. Removing the columns in $\mathbf{H}_0$, which is linearly dependent on the columns in $\mathbf{H}$, we have $\mathbf{H}_0^d = h_{0,1}$, i.e., $r([\mathbf{H}_0^d\ \mathbf{H}]) = n = 3$ and $h_{0,1} \neq \sum_{i\notin S^d} \Delta\theta_i \cdot h_{0,i} + \sum_{j\in\mathcal{N}_{-r}} \theta_j \cdot h_j$. Then for any specific FDI attacks $\mathbf{a} = \mathbf{H}_0 \cdot \Delta\boldsymbol{\theta}$, $\Delta\boldsymbol{\theta} \in R^2$, $\Delta\theta_1 \neq 0$, $\mathbf{a}$ cannot be expressed as the weighted sum of the columns in $\mathbf{H}$, i.e., $\mathbf{a}$ is not in the column space of $\mathbf{H}$, and any specific FDI attacks $\mathbf{a} = \mathbf{H}_0 \cdot \Delta\boldsymbol{\theta}$, $\Delta\theta_1 \neq 0$ can be detected.

As described in Theorem 2, FDI attacks $\mathbf{a} = \mathbf{H_0} \cdot \Delta\boldsymbol{\theta}$, where $\Delta\theta_i \neq 0$, $i \in S^d$, can be detected if $r([\mathbf{H}_0^d\ \mathbf{H}\ ]) = n - 1 + |S^d|$. The relationship between the probability of detecting FDI attacks and the rank of the composite matrix can be expressed as follows.

Remark 3: For a given composite matrix satisfying $r([\mathbf{H}_0^d\ \mathbf{H}]) = n - 1 + |S^d|$, the probability of detecting FDI attacks increase when the number of attacked state increases, and the probability of detecting FDI attacks increase when the rank of the composite matrix increases.

That is, for a given $|S^d|$, satisfying $r([\mathbf{H}_0^d\ \mathbf{H}]) = n - 1 + |S^d|$, the detection probability increases when $\|\Delta\boldsymbol{\theta}\|_0$ increases, and for a given number of attacked states, i.e., $\|\Delta\boldsymbol{\theta}\|_0$, the detection probabilities increases when $|S^d|$ increases.

Partial FDI attacks can also be identified by the new matrix $\mathbf{H}$ in secure reactance perturbation even though the composite matrix is not full column rank. The identification condition for specific attack can be described as

Theorem 3 (Partial Attack Identification Condition): For a given composite matrix $[\mathbf{H}_0\ \mathbf{H}]$, $\mathbf{H}_0, \mathbf{H} \in R^{m\times(n-1)}$, suppose S^i is an index set of some columns in $\mathbf{H}_0$, such that $r([\mathbf{H}_0^i\ \mathbf{H}]) = n - 1 + |S^i|$, where $\mathbf{H}_0^i$ is the matrix consisting of columns in $\mathbf{H}_0$ indexed by S^i, and $|S^i|$ is the cardinality of set S^i. Specific FDI attacks $\mathbf{a} = \mathbf{H}_0 \cdot \Delta\boldsymbol{\theta}$, $\Delta\boldsymbol{\theta} \in R^{n-1}$, can be identifiable if for any $i \notin S^i$, $\Delta\theta_i = 0$.

Proof: For specific FDI attacks $\mathbf{a} = \mathbf{H}_0 \cdot \Delta\boldsymbol{\theta}$, $\Delta\boldsymbol{\theta} \in R^{n-1}$, $\forall i \notin S^i$, $\Delta\theta_i = 0$, the compromised measurement in (10) can be reformulated as:

$$\mathbf{z_a} = \begin{bmatrix} \mathbf{H}_0^i & \mathbf{H} \end{bmatrix} \cdot \begin{bmatrix} \Delta\boldsymbol{\theta}^i \\ \boldsymbol{\theta} \end{bmatrix}, \tag{19}$$

where $\mathbf{H}_0^i$ consists of the columns in $\mathbf{H}_0$ indexed by S^i, and $\Delta\boldsymbol{\theta}^i \in R^{|S^i|}$ composed of $\Delta\theta_i$, $i \in S^i$. As $r([\mathbf{H}_0^i\ \mathbf{H}]) = n - 1 + |S^i|$, $[\Delta\boldsymbol{\theta}^{i^T}\ \Delta\boldsymbol{\theta}^T]^T \in R^{n-1+|S^i|}$, i.e., matrix $[\mathbf{H}_0^i\ \mathbf{H}]$ is invertible. Hence any vector $[\Delta\boldsymbol{\theta}^{i^T}\ \Delta\boldsymbol{\theta}^T]^T$ can be calculated accurately. That is, $\mathbf{a} = \mathbf{H}_0 \cdot \Delta\boldsymbol{\theta}$, $\forall i \notin S^i$, $\Delta\theta^i = 0$ can be identified. ■

As described in Theorem 3, FDI attacks can be identified by the composite matrix, satisfying $r([\mathbf{H}_0^i\ \mathbf{H}]) = n - 1 + |S^i|$, if $\forall i \notin S^i$, $\Delta\theta_i = 0$. The relationship between the identification probability and the number of attacked states can be described as follows:

Remark 4: For a composite matrix, satisfying $r([\mathbf{H}_0^i\ \mathbf{H}]) = n - 1 + |S^i|$, the probability of identifying FDI attacks decreases when the number of attacked states increases, and the probability of identifying FDI attacks increases when $|S^i|$ increases.

That is, for a given $|S^i|$, the identification probability decreases when $\|\Delta\boldsymbol{\theta}\|_0$ increases, and for a given number of attacked states $\|\Delta\boldsymbol{\theta}\|_0$, the identification probability increases when $|S^i|$ increases.

Even though Theorem 1, 2 and 3 are deduced based on FDI attacks in DC state estimation, such conclusions can be generalized to FDI attacks constructed based on linearized power flow model [16], [18] by replacing the measurement matrix $\mathbf{H}$ with locally linearized measurement matrices of the nonlinear power flow equations, where such attacks can hardly be detected by bad data detection in nonlinear AC state estimation without reactance perturbation.

As defined in Theorems 2 and 3, S^d is the index set of columns in $\mathbf{H}_0$ excluding those linearly dependent on the columns of $\mathbf{H}$, and S^i is a index set of some columns in $\mathbf{H}_0$, such that $r([\mathbf{H}_0^i\ \mathbf{H}]) = n - 1 + |S^i|$, we have columns in $\mathbf{H}_0$, $h_{0,i}$, $i \notin S^d$, is linearly dependent on columns in $\mathbf{H}$, and $h_{0,i}$, $i \in S^i$, is linearly independent on columns in $\mathbf{H}$. There might be columns in $\mathbf{H}_0$, $h_{0,i}$ and $h_{0,j}$, such that $h_{0,i}$ and $h_{0,j}$ are linearly independent on columns in $\mathbf{H}$, respectively, while $h_{0,i}$, $h_{0,j}$ and columns in $\mathbf{H}$ are not linear independent. That is, for a given composite matrix $\mathbf{M}$, columns in $\mathbf{H}_0$ can be divided into 3 groups, columns outside of S^d, i.e., columns in $\mathbf{H}_0$ linearly dependent on columns in $\mathbf{H}$, columns in S^i, i.e., columns in $\mathbf{H}_0$ linearly independent on columns in $\mathbf{H}$, and columns in $S^d \backslash \{S^i\}$. As there might be columns, linearly independent on columns in $\mathbf{H}$ while not linearly independent on columns in $\mathbf{H}_0^i$ and $\mathbf{H}$, we have $r([\mathbf{H}_0^d\ \mathbf{H}]) \neq n - 1 + |S^d|$ when $S^d \backslash S^i \neq \emptyset$. That is, $r([\mathbf{H}_0^d\ \mathbf{H}]) = n - 1 + |S^d|$ does not always holds for all the possible composite matrices.

For a composite matrix $\mathbf{M}$ where $S^d \backslash S^i \neq \emptyset$, attack vector $\mathbf{a} = \mathbf{H}_0 \cdot \Delta\boldsymbol{\theta}$ can be decomposed as $\sum_{i \notin S^d} \Delta\theta_i \cdot h_{0,i} + \sum_{i \in S^i} \Delta\theta_i \cdot h_{0,i} + \sum_{i \in S^d \backslash S^i} \Delta\theta_i \cdot h_{0,i}$. As columns $h_{0,i}$, $i \notin S^d$ depend on columns in $\mathbf{H}$, there exists θ such that $\sum_{i \notin S^d} \Delta\theta_i \cdot h_{0,i} = \sum_{j \in \mathcal{N}_{-r}} \theta_j \cdot h_j$. As the columns in $S^d \backslash S^i$ depend on columns in $[\mathbf{H}_0^i\ \mathbf{H}]$, there exists $\Delta\boldsymbol{\theta}'$ and $\boldsymbol{\theta}'$ such that

$$\sum_{i \in S^d \backslash S^i} \Delta\theta_i \cdot h_{0,i} = \sum_{i \in S^i} \Delta\theta_i' \cdot h_{0,i} + \sum_{j \in \mathcal{N}_{-r}} \theta_j' \cdot h_j.$$

That is, FDI attacks $\mathbf{a} = \mathbf{H}_0 \cdot \Delta\boldsymbol{\theta}$, where $\Delta\theta_i \neq 0$, $i \in S^d$, can be expressed as

$$\begin{aligned}\mathbf{a} &= \sum_{i \notin S^d} \Delta\theta_i \cdot h_{0,i} + \sum_{i \in S^i} \Delta\theta_i \cdot h_{0,i} + \sum_{i \in S^d \backslash S^i} \Delta\theta_i \cdot h_{0,i} \\ &= \sum_{i \in S^i} (\Delta\theta_i + \Delta\theta_i') \cdot h_{0,i} + \sum_{j \in \mathcal{N}_{-r}} (\theta_j + \theta_j') \cdot h_j.\end{aligned}$$

This means that there might be FDI attacks $\mathbf{a} = \mathbf{H}_0 \cdot \Delta\boldsymbol{\theta}$, $\Delta\theta_i \neq 0$, $i \in S^d$, where changes in states introduced by attack vector $\mathbf{a}$ are well coordinated, such that $\Delta\boldsymbol{\theta} + \Delta\boldsymbol{\theta}' = 0$ when $r([\mathbf{H}_0^d\ \mathbf{H}]) = n - 1 + |S^d|$ does not hold, i.e., the attack vector $\mathbf{a}$ is in the column space of $\mathbf{H}$ and $\mathbf{a}$ cannot be detected by the new matrix in reactance perturbation. However, as the attacker does not know the exact value of $\mathbf{H}$, it is hard to coordinate the injected attack vector such that the attack vector is undetectable. Hence, we have the following remark.

Remark 5: Most of FDI attacks $\mathbf{a} = \mathbf{H}_0 \cdot \Delta\boldsymbol{\theta}$, $\Delta\theta_i \neq 0$, $i \in S^d$, can still be detected even though $r([\mathbf{H}_0^d\ \mathbf{H}]) \neq n - 1 + |S^d|$, where S_d is the index set of rest columns in $\mathbf{H}_0$ by removing columns linearly depending on columns in $\mathbf{H}$.

That is, Theorem 2 can be relaxed and FDI attacks $\mathbf{a} = \mathbf{H}_0 \cdot \Delta\boldsymbol{\theta}$ can be detected by the new matrix $\mathbf{H}$ in reactance perturbation in most of cases if there exits $\Delta\theta_i \neq 0$, $i \in S^d$, even though $r([\mathbf{H}_0^d\ \mathbf{H}]) \neq n - 1 + |S^d|$.

As described in Remark 3 and the description above, the probability of detecting FDI attack increases when the rank of the composite matrix $[\mathbf{H}_0\ \mathbf{H}]$ increases, because $r([\mathbf{H}_0^d\ \mathbf{H}]) = r([\mathbf{H}_0\ \mathbf{H}])$. As $r([\mathbf{H}_0^i\ \mathbf{H}]) \leq r([\mathbf{H}_0\ \mathbf{H}])$, a composite matrix with a larger rank maybe increase the rank of $[\mathbf{H}_0^i\ \mathbf{H}]$, and the probability of identifying FDI attacks may increase when the rank of the composite matrix increases (Remark 4). Hence, we maximize the rank of the composite matrix in secure reactance perturbation optimization to maximize the probability of detecting FDI attacks.

IV. Secure Reactance Perturbation Optimization and Monitor Design

In this section, we formulate an optimization for secure reactance perturbation and design a heuristic algorithm to jointly optimize the rank of the composite matrix and the power losses introduced by reactance perturbation. An monitor is designed, which uses the composite matrix obtained from secure reactance perturbation optimization to detect and identify FDI attacks.

A. Secure Reactance Injection Optimization

In power system state estimation, a defender aims to maximize the probability of detecting FDI attacks and minimize the power losses introduced by reactance perturbation. Hence, the secure reactance perturbation problem (SRPP) can be formulated as:

$$\begin{aligned}&\min_{\Delta \boldsymbol{x}} -\alpha \cdot r(\mathbf{M}) + LS \cdot \Delta\mathbf{x} \\ &\text{s.t. } (3), (4),\end{aligned}$$

where (3) and (4) are constraints on reactance perturbation, $LS \cdot \Delta\mathbf{x}$ is the power losses introduced by reactance perturbation, and $\mathbf{M}$ is the composite matrix as defined in (16). In order to maximize the probability of detecting and identifying FDI attacks in priority, the multiplier α must be positive and sufficiently large.

There are difficulties in solving the SRPP above, because 1) we maximize the rank of the matrix (nonconvex) in SRPP. It cannot be relaxed to maximize the nuclear norm [30] as in minimizing matrix rank problems; 2) there are logical "OR"s in constraint (4), which is nonconvex. Hence, the SRPP cannot be solved directly.

Take the composite matrix $\mathbf{M}$ as a variable matrix [28], where the entries in $\mathbf{H}_0$ are fixed and entries in $\mathbf{H}$ can be changed, the SRPP is a special case in maximum rank matrix completion (MRMC) problems. Inspired by the MRMC algorithm in [28], we can maximize the rank of the composite matrix by updating transmission line's reactance one by one. Denote the composite matrix as $\mathbf{M}(x_{ij})$ and $\mathbf{M}(x_{ij}')$ with the reactance of transmission line ij, x_{ij} and x_{ij}', respectively. For a composite matrix $\mathbf{M}$, we have the follow theorem:

Theorem 4: For a composite matrix $\mathbf{M}$, $r(\mathbf{M}(x_{ij})) < \min\{m, 2 \cdot (n-1)\}$, as defined in (16), if the rank of the matrix increase when changing the reactance on transmission line, connecting bus i and j, from x_{ij} to x_{ij}', $x_{ij}' \neq x_{ij}$, i.e., $r(\mathbf{M}(x_{ij}')) > r(\mathbf{M}(x_{ij}))$, then for any value of reactance on transmission line connecting bus i and j, $x''_{ij} \neq x'_{ij} \neq x_{ij}$, we have $r(\mathbf{M}(x''_{ij})) > r(\mathbf{M}(x_{ij}))$.

Proof: Suppose $r(\mathbf{M}(x_{ij})) = K$, $K < \min\{m, 2 \cdot (n-1)\}$. Denote the row index set of $\mathbf{M}(x_{ij})$ as V_r, and the column index set as V_c. Let $\mathbf{M}^{\mathrm{s}}(x_{ij})$ be the sub-matrix composed of elements indexed by set ν_r and ν_c, where $|\nu_r| = K+1, \nu_r \in V_r$, and $|\nu_c| = K+1$, $\nu_c \in V_c$, i.e., $\mathbf{M}^{\mathrm{s}}(x_{ij}) = \mathbf{M}(x_{ij})_{[\nu_r, \nu_c]}$, $r(\mathbf{M}^{\mathrm{s}}(x_{ij})) \leq K$.

We analyze the determinant of $\mathbf{M}^{\mathrm{s}}(x_{ij})$ for the following two cases: 1) There are no nonzero elements, related to x_{ij}, in $\mathbf{M}^{\mathrm{s}}(x_{ij})$; 2) There are nonzero elements, related to x_{ij}, in $\mathbf{M}^{\mathrm{s}}(x_{ij})$, which can be denoted as $h_{ij}, \ldots, h_{k\ell}$.

For any sub-matrix $\mathbf{M}^{\mathrm{s}}(x_{ij})$ in case 1), we have: for any $x'_{ij} \neq x_{ij}$, $\det(\mathbf{M}^{\mathrm{s}}(x'_{ij})) = \det(\mathbf{M}^{\mathrm{s}}(x_{ij})) = 0$. This means that in case 1), $r(\mathbf{M}^{\mathrm{s}}(x'_{ij})) \leq K$.

For any sub-matrix $\mathbf{M}^{\mathrm{s}}(x_{ij})$ in case 2), the determinant of $\mathbf{M}^{\mathrm{s}}(x_{ij})$ can be expressed as [28]:

$$\begin{aligned} \det(\mathbf{M}^{\mathrm{s}}(x_{ij})) &= 1/x_{ij} \cdot (\beta \cdot \det(\mathbf{M}^{\mathrm{s}}(x_{ij})_{[\nu_r \backslash \{i\}, \nu_c \backslash \{j\}]}) + \cdots \\ &\quad + \lambda \cdot \det(\mathbf{M}^{\mathrm{s}}(x_{ij})_{[\nu_r \backslash \{k\}, \nu_c \backslash \{\ell\}]})) + \det(\mathbf{M}^{\mathrm{s}}(\infty)) + b = 0, \end{aligned} \tag{20}$$

where $\mathbf{M}^{\mathrm{s}}(\infty)$ is the matrix replacing x_{ij} with ∞, b is a constant. Obviously, for sub-matrix in case 2), $\det(\mathbf{M}^{\mathrm{s}}(x_{ij}))$ is a linear function of $1/x_{ij}$. When the multiplier of $1/x_{ij}$ is nonzero, there is only one solution to $\det(\mathbf{M}^{\mathrm{s}}(x_{ij})) = 0$, i.e., for any $x'_{ij} \neq x_{ij}$, $\det(\mathbf{M}^{\mathrm{s}}(x'_{ij})) \neq 0$, and $r(\mathbf{M}^{\mathrm{s}}(x'_{ij})) = K+1$. Else, the multiplier of $1/x_{ij}$ is zero, and for any $x'_{ij} \neq x_{ij}$, $\det(\mathbf{M}^{\mathrm{s}}(x'_{ij})) = 0$, i.e., $r(\mathbf{M}^{\mathrm{s}}(x'_{ij})) \leq K$.

In conclusion, if the multiplier of $1/x_{ij}$ in $\det(\mathbf{M}^{\mathrm{s}}(x_{ij}))$ is nonzero, for any $x'_{ij} \neq x_{ij}$, we have $r(\mathbf{M}^{\mathrm{s}}(x'_{ij})) > K \geq r(\mathbf{M}^{\mathrm{s}}(x_{ij}))$. Else, for any $x'_{ij} \neq x_{ij}$, we have $r(\mathbf{M}^{\mathrm{s}}(x'_{ij})) \leq K$. As $r(\mathbf{M}(x'_{ij})) = \max\{\mathbf{M}(x'_{ij})_{[\nu_r, \nu_c]} | \nu'_r \in V_r, \nu'_c \in V_c, |\nu'_r| \geq K+1, |\nu'_c| \geq K+1\}$, if there exist $x'_{ij} \neq x_{ij}$ such that $r(\mathbf{M}(x'_{ij})) > r(\mathbf{M}(x_{ij})) = K$, there exist sub-matrix $\mathbf{M}^{\mathrm{s}}(x_{ij})$, such that $r(\mathbf{M}^{\mathrm{s}}(x'_{ij})) > K \geq r(\mathbf{M}^{\mathrm{s}}(x_{ij}))$. Then for any $x''_{ij} \neq x_{ij}$, $r(\mathbf{M}(x''_{ij})) \geq r(\mathbf{M}^{\mathrm{s}}(x''_{ij})) > K$. Hence, the theorem holds. ■

As described in Theorem 4, if the rank of the composite matrix increases when we change branch reactance from x_{ij} to x'_{ij}, $x'_{ij} \neq x_{ij}$, any other reactance $x''_{ij} \neq x'_{ij} \neq x_{ij}$ can ensure the increase in the rank of the composite matrix. Moreover, Theorem 4 provides an algorithm to find a maximum rank completion. Indeed, suppose the rank of the current matrix is K, i.e., $r(\mathbf{M}) = K$, $K \leq \min\{m, 2 \cdot (n-1)\}$, one could change elements in $\mathbf{x}$ one by one and check the rank of the new matrix. If the rank of the matrix increases by changing $x_{k\ell}$, update $x_{k\ell}$ with $x_{k\ell} + \Delta x_{k\ell}$ and change the other elements to increase rank repeatedly. If there is no element in $\mathbf{x}$ to increase the rank or $r(\mathbf{M}) = \min\{m, 2 \cdot (n-1)\}$, stop the iteration. In each iteration, we check at most p times, and after at most $n-1$ iterations (from $n-1$ to $2 \cdot (n-1)$), the algorithm stops. That is, the algorithm stops in polynomial time.

As the rank of the composite matrix is related to all the entries, in each iteration, the decision on Δx_{ij} is related to all the previous decisions on $\Delta \mathbf{x}$; we cannot separate the rank increasing and cost minimizing process, i.e., we cannot maximize the rank first and minimize the operational cost in the end. Therefore, in the kth iteration, if it will increase the rank of the matrix by changing x_{ij}, we solve the following subproblem (SP):

$$\begin{aligned} \min_{\Delta \mathbf{x}^{(k)}} \quad & LS(\mathbf{x}^{(k)}) \cdot \Delta \mathbf{x}^{(k)} \\ \text{s.t.} \quad & (1+\underline{\tau}) \cdot x_{0ij} \leq \Delta x_{ij}^{(k)} + x_{ij}^{(k)} \leq (1+\overline{\tau} \cdot x_{0ij}), \\ & |\Delta x_{ij}^{(k)}| \geq \omega \cdot |x_{0ij}|, \\ & \Delta x_{-ij}^{(k)} = \mathbf{0}, \end{aligned} \tag{21}$$

where $LS(\mathbf{x}^{(k)})$ is the linear sensitivity matrix on the current state $\mathbf{x}^{(k)}$ in the kth iteration, $x_{-ij}^{(k)}$ are other elements in $\mathbf{x}^{(k)}$ except $x_{ij}^{(k)}$, and x_{0ij} is the original line reactance, i.e., transmission line's reactance when there is no D-FACTS devices. After changing reactance, the sensitivity matrix LS need to be updated. The secure reactance perturbation algorithm is presented in Algorithm 1.

Algorithm 1: Secure Reactance Perturbation Algorithm.

```
Input: $\mathbf{D}$, $\mathbf{X}_0$, $\mathbf{A}$, and $\mathbf{x}_0$
Initialization: $\mathbf{X} = \mathbf{X}_0$, $\mathbf{x} = \mathbf{x}_0$,
    $\mathbf{M} = \mathbf{D} \cdot \begin{bmatrix} \mathbf{X}_0 & \mathbf{X} \end{bmatrix} \cdot \begin{bmatrix} \mathbf{A}_{-r}^T & 0 \\ 0 & \mathbf{A}_{-r}^T \end{bmatrix}$;
while $r(\mathbf{M}) < 2 \cdot (n-1)$
    $F = 0$;
    for each $ij \in \mathcal{A}$
        $\Delta x_{ij} = \overline{\tau} \cdot x_{ij}$;
        $x_{ij} = x_{ij} + \Delta x_{ij}$;
        $\mathbf{M}' = \mathbf{D} \cdot \begin{bmatrix} \mathbf{X}_0 & \mathbf{X} \end{bmatrix} \cdot \begin{bmatrix} \mathbf{A}_{-r}^T & 0 \\ 0 & \mathbf{A}_{-r}^T \end{bmatrix}$;
        if $r(\mathbf{M}') > r(\mathbf{M})$;
            $F = 1$;
            $\Delta x_{ij} = \arg\min LS \cdot \Delta \mathbf{x}$; % solve the subproblem SP
            $x_{ij} = x_{ij} + \Delta x_{ij}$; % update reactance vector
    $x$.
            $LS = LS(\mathbf{x})$; % update linear sensitivity matrix.
            $\mathbf{X} = diag(1./\mathbf{x})$; % update diagonal reactance matrix $X$.
            $\mathbf{M} = \mathbf{D} \cdot \begin{bmatrix} \mathbf{X}_0 & \mathbf{X} \end{bmatrix} \cdot \begin{bmatrix} \mathbf{A}_{-r}^T & 0 \\ 0 & \mathbf{A}_{-r}^T \end{bmatrix}$;
            break;
        end
    end
    if $F == 0$
        break;
    end
end
Output: $\mathbf{x}$, $\mathbf{M}$
```

As shown in Algorithm 1, the input consists of the sensor deployment matrix $\mathbf{D}$, original diagonal branch reactance matrix $\mathbf{X}_0$, and topology incidence matrix $\mathbf{A}$. The output of the algorithm is given by the final branch reactance vector $\mathbf{x}$ and composite matrix $\mathbf{M}$. At initialization, we let $\mathbf{X} = \mathbf{X}_0$, $\mathbf{x} = \mathbf{x}_0$, and generate an original composite matrix. In lines 2-21, we increase the rank of the matrix by changing the entries of $\mathbf{x}$ one after another when $r(\mathbf{M}) < 2 \cdot (n-1)$. F is a flag used to record the increase of the rank when changing x_{ij}, $ij \in \mathcal{A}$. The algorithm stops if the rank of the new matrix does not increase by changing all entries in $\mathbf{x}$ one by one. That is, the algorithm stops if the algorithm cannot increase the rank of the composite matrix any further. If the rank of the matrix increases when changing entry in $\mathbf{x}$ from x_{ij} to $x_{ij} + \Delta x_{ij}$, we solve the subproblem of SRPP in line 10 to obtain the optimal reactance perturbation Δx_{ij}. Linear sensitivities matrix is updated on line 12.

As we minimize operational cost at each iteration, the final operational cost may be related to the searching sequence of x_{ij}, and the final operational cost may not be the global optimum. Moreover, the secure reactance perturbation algorithm above cannot ensure the maximal rank as the rank may not increase by changing only one of the entries of $\mathbf{x}$ as discussed in [28].

B. Monitor for Detecting and Identifying FDI Attacks

In this part, we design a monitor to detect and identify FDI attacks in both noiseless and noisy systems, where the input of the monitor is the previous measurement matrix $\mathbf{H}_0$, the new measurement matrix in secure reactance perturbation $\mathbf{H}$, and the compromised measurement $\mathbf{z_a}$, while the output is the detection result and the value of identified attack vector.

As discussed in Section III, any FDI attacks can be detected in noiseless case if attack vector $\mathbf{a} = \mathbf{H}_0 \cdot \Delta\boldsymbol{\theta}$ is not in the column space of the new measurement matrix $\mathbf{H}$, i.e., $\mathbf{a} \notin C(\mathbf{H})$. As the real measurement $\mathbf{z} = \mathbf{H} \cdot \boldsymbol{\theta}$ is within the column space of $\mathbf{H}$, we can easily detect the originally covert FDI attacks in reactance perturbation by checking if the compromised measurement is within the column space of the new measurement matrix $\mathbf{H}$. Specifically, the detection result is

$$\psi(\boldsymbol{\Lambda}) = \begin{cases} \text{True} & r([\mathbf{H}\ \mathbf{z_a}]) > r(\mathbf{H}), \\ \text{False} & \text{otherwise.} \end{cases} \tag{22}$$

As the accuracy of the detection strategy above may be affected by measurement noise, which is usually exist in practice, a new detection method need to be designed in systems with measurement noise. In systems with measurement noise, we design a measurement residual based detection strategy in reactance perturbation. Specifically, the monitor alarms, i.e., $\psi_1(\boldsymbol{\Lambda}) = \text{True}$, when the measurement residual satisfies:

$$\|\mathbf{z_a} - \mathbf{H} \cdot (\mathbf{H}^T \cdot \mathbf{H})^{-1} \cdot \mathbf{H}^T \cdot \mathbf{z_a}\|^2 > \gamma^2,$$

where γ is a preset threshold related to the detection confidence probability.

Based on Theorem 3, changes in voltage phase angles, i.e., system states, introduced by attack vector $\mathbf{a}$ in both noiseless and noisy systems, can be estimated as:

$$\begin{bmatrix} \Delta\hat{\boldsymbol{\theta}}^i \\ \hat{\boldsymbol{\theta}} \end{bmatrix} = \left(\left[\mathbf{H}_0^i\ \mathbf{H}\right]^T \cdot \left[\mathbf{H}_0^i\ \mathbf{H}\right] \right)^{-1} \cdot \left[\mathbf{H}_0^i\ \mathbf{H}\right]^T \cdot \mathbf{z_a}.$$

Using the estimated changes in system states, the identified attack vector, i.e., $\psi_2(\boldsymbol{\Lambda})$, can be calculated as:

$$\psi_2(\boldsymbol{\Lambda}) = \mathbf{H} \cdot \begin{bmatrix} \Delta\hat{\boldsymbol{\theta}}^i \\ \mathbf{0} \end{bmatrix},$$

where $\mathbf{0}$ denotes that the changes of states, outside of the index set S^i, are assumed to be zeros.

V. Numerical Simulation

We empirically explore the performance of attack mitigation in both noiseless and noisy cases, and the effect of secure reactance perturbation on power losses. A 6-bus power system [31], and the IEEE 57-bus test system [32] are used in our case studies. We assume that all test systems are fully measured. Other configuration data, such as branch impedance, transmission lines' power flow limits, and generation limits, are obtained from the MATPOWER packages [33]. Linear sensitivities matrices are calculated based on the parameters above, and are updated once line reactance changes. Load demand is given and assumed to be constant. The constraints on the changes in line reactance are set to $\underline{\tau} = -10\%$, $\overline{\tau} = 10\%$, and $\omega = 5\%$.

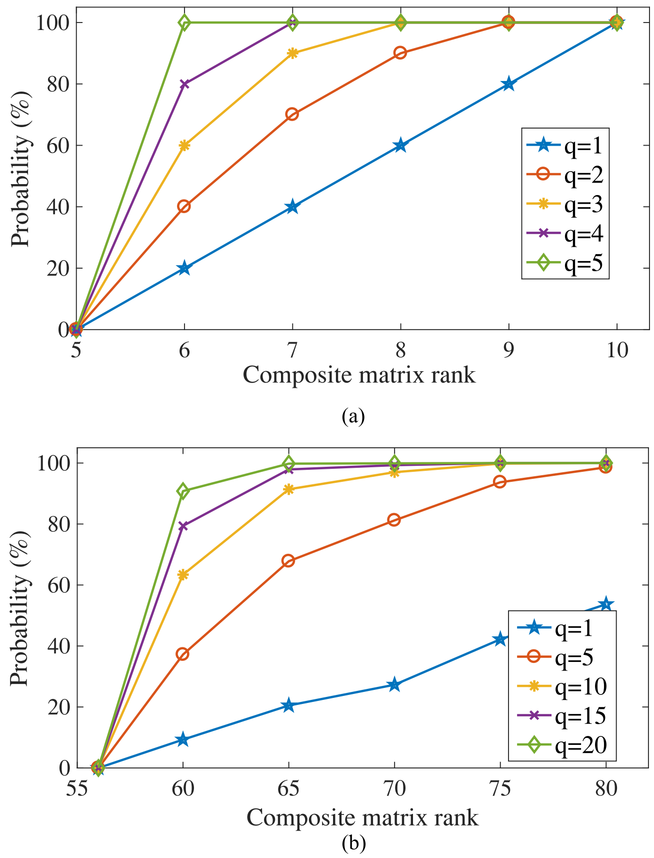
In order to verify the relationship amongst detection/identification probabilities, the number of modified state, and the rank of composite matrix, we simulate the detection and identification of FDI attacks in the 6-Bus power system and the IEEE 57-Bus power system with noiseless setting. In each simulation, we generate $\Delta\boldsymbol{\theta}$ randomly with a fixed number of modified states, i.e., $\|\Delta\boldsymbol{\theta}\|_0 = q$, $q = 1, \ldots, n-1$, and inject attack vector $\mathbf{a} = \mathbf{H}_0 \cdot \Delta\boldsymbol{\theta}$ is injected into the real measurement $\mathbf{H} \cdot \boldsymbol{\theta}$, where $\boldsymbol{\theta}$ is randomly generated. For a given number of modified states, we simulate the case 1000 times to average the probability of detecting and identifying FDI attacks.

As discussed in Section IV-B, FDI monitor alarms when the compromised measurement are not in the column space of the new measurement $\mathbf{H}$, and FDI attacks are detected successfully when $\psi_1(\boldsymbol{\Lambda}) = \textit{True}$ and attack vector $\mathbf{a} \neq \mathbf{0}$. Moreover, FDI attacks are identified exactly if the deviation between the attack vector $\mathbf{a}$ and the estimated attack vector $\hat{\mathbf{a}}$ is no larger than a preset threshold ε, i.e.,

$$\frac{\|\mathbf{a} - \hat{\mathbf{a}}\|_2}{\|\mathbf{a}\|_2} \cdot 100\% \leq \varepsilon. \tag{23}$$

Here, $\varepsilon = 5\%$. The probabilities of detecting and identifying FDI attacks in the noiseless 6-bus and 57-bus power systems are given in Figs. 2 and 3.

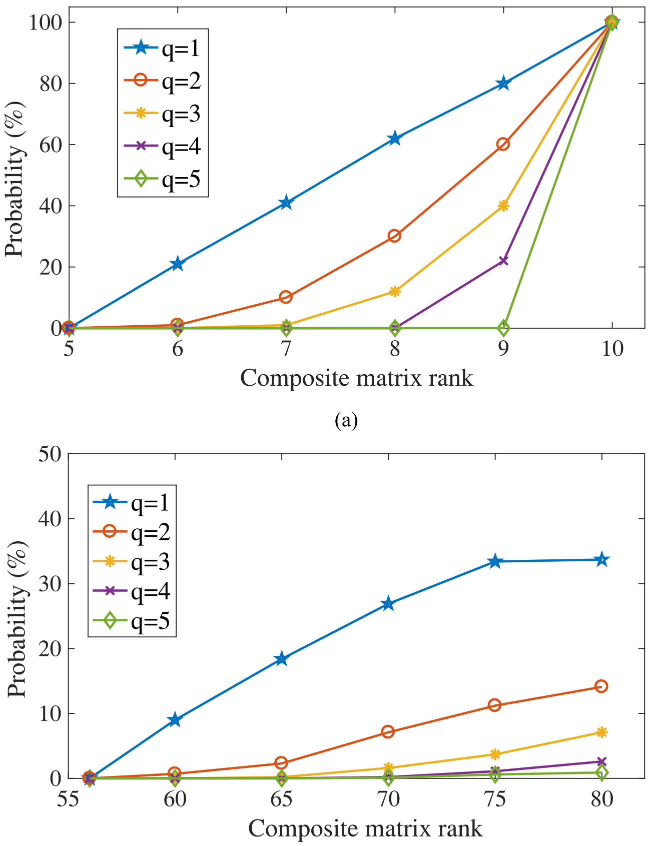
As shown in Fig. 2, the detection probabilities of FDI attacks increase significantly with the increase of the composite matrix's rank and the detection probabilities increase when the number of attacked states increases. The reason is that the monitor can detect FDI attacks $\mathbf{a} = \mathbf{H}_0 \cdot \Delta\boldsymbol{\theta}$, where $\Delta\theta_i \neq 0$, $i \in S^d$, and the probability of detecting FDI attacks increase when $|S^d|$ increase; here, the rank of $\mathbf{M}$ increases, or $\|\Delta\boldsymbol{\theta}\|_0$ increases, i.e., the number of the attacked states increases. No FDI attack can be detected without reactance perturbation, i.e., $r(\mathbf{M}) = n - 1$, and all FDI attacks can be detected in the 6-bus system when



(a)

(b)

Fig. 2. Probabilities of detecting FDI attacks in noiseless power systems. (a) Detection probabilities in the noiseless 6-bus system. (b) Detection probabilities in the noiseless 57-bus system.



(a)

(b)

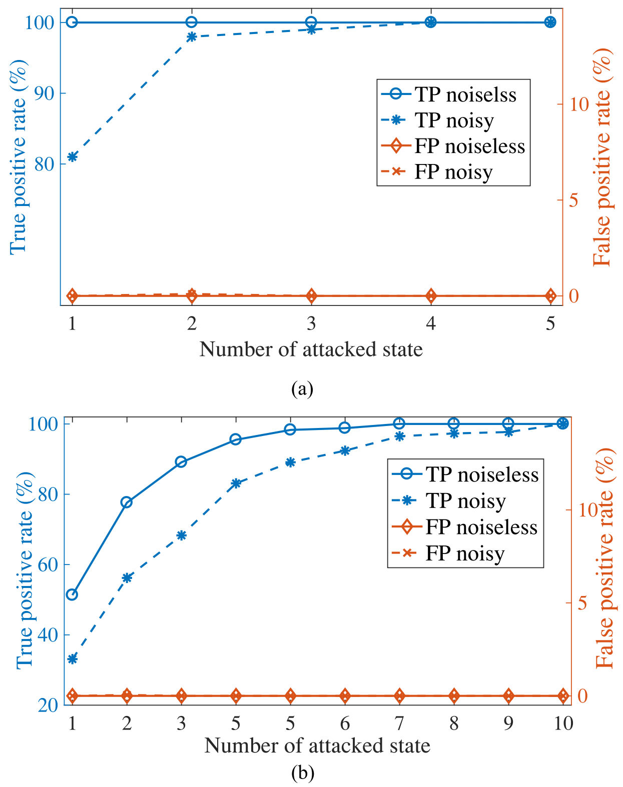
Fig. 3. Probabilities of identifying FDI attacks in noiseless power systems. (a) Identification probabilities in the noiseless 6-bus system. (b) Identification probabilities in the noiseless 57-bus system.

the composite matrix is full column rank. Constrained by the system topology ($p = 80 \leq 2 \cdot (n-1)$), the composite matrix in the IEEE 57-Bus power system is not full column rank, and the probability of detecting FDI attacks, with a fixed number of attacked state $q = 1$, is no larger than 60%.

As shown in Fig. 3, the probabilities of identifying FDI attacks increase with the increase of the composite matrix's rank. Different from the probabilities of detecting FDI attacks in reactance perturbation, the probabilities of identifying FDI attacks decrease when the number of attacked states increases. The reason is that monitor can only identify FDI attacks $\mathbf{a} = \mathbf{H}_0 \cdot \Delta\boldsymbol{\theta}$, where for any $i \notin S^i$, $\Delta\theta_i = 0$, and the probabilities of identifying FDI attacks decrease when $\|\Delta\boldsymbol{\theta}\|_0$ increases, i.e., the number of the attacked meters increases. Similar to the probabilities of detecting FDI attacks, the original covert FDI attacks cannot be identified when there is no reactance perturbation, i.e., $r(\mathbf{M}) = n-1$, and all FDI attacks can be identified in the 6-bus system when the composite matrix is full column rank. The probability of identifying FDI attacks is no larger than 40% in the 57-bus system, because of the limits on power system topology. FDI attacks can hardly be identified when the number of attacked meters is more than 5, i.e., $q \geq 5$, because there exists $i \notin S^i$, $\Delta\theta_i \neq 0$ with a high probability and Theorem 3 is not satisfied.

In order to verify the effect of measurement noise on the performance of attack detection and identification, we compare the detection and identification probabilities in noiseless and noisy cases. In systems with measurement noise, zero mean Gaussian distribution noises are introduced in the compromised measurements, i.e., $\mathbf{z_a} = \mathbf{H} \cdot \boldsymbol{\theta} + \mathbf{H}_0 \cdot \Delta\boldsymbol{\theta} + \mathbf{e}$, where the standard deviation of the ith meter is $\sigma_i = 0.01$ p.u. [34]. In systems with measurement noise, FDI monitor alarms when the measurement residual is larger than a preset threshold γ, which is set to $\gamma = 0.1$ here. We simulate with the maximal rank of the composite matrix, i.e., $r(\mathbf{M}) = 10$ in the 6-bus system and $r(\mathbf{M}) = 80$ in the IEEE 57-bus test system. To verify the effect of measuremen noises on detection probablities, we record the true positive (TP) rate when there are FDI attacks and measurement noises, and the false positive (FP) rate when there are measurement noises without attacks. For a given number of attacked state, i.e., $\|\mathbf{a}\|_0 = q$, $q = 1, \ldots, n-1$, we simulate 1000 times to average TP rate and FP rate. The attack detection probabilities in 6-bus and 57-bus power systems are given in Fig. 4.

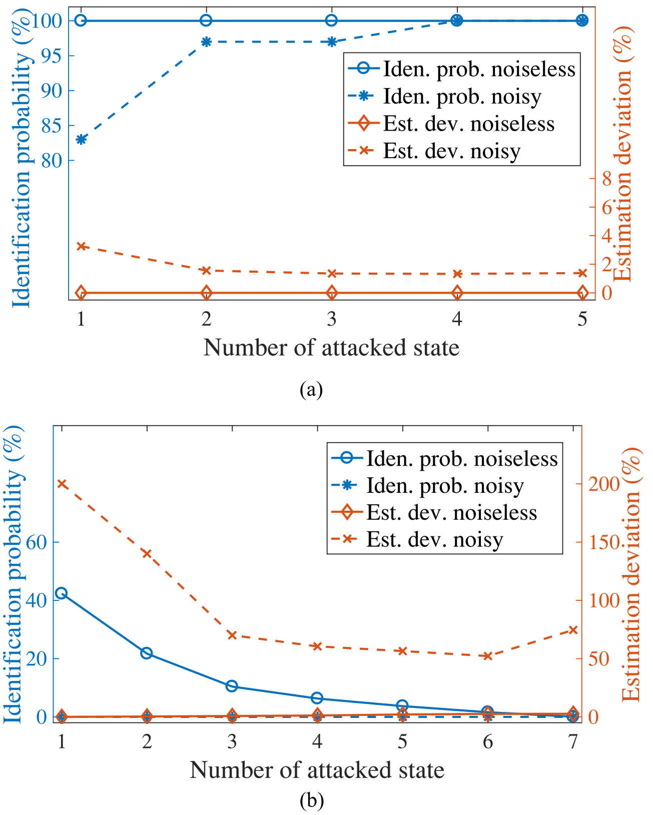
As shown in Fig. 4, the probabilities of detecting FDI attacks increase with the number of attacked state in both noiseless and noisy cases. The true positive rate in noisy cases is a little lower than that in noiseless systems, and the deviation in true posi-



(a)

(b)

Fig. 4. Probabilities of detecting FDI attacks in noiseless and noise cases. (a) Detection probabilities in the 6-bus system, *r(M)* = 10. (b) Detection probabilities in the 57-bus system, *r(M)* = 80.



(a)

(b)

Fig. 5. Probabilities of identifying FDI attacks in noiseless and noise cases. (a) Identification probabilities in the 6-bus system. (b) Identification probabilities in the 57-bus system.

tive rate decreases with the increase of the number of attacked state. In the 6-bus system, the true positive rate is more than 95% when the number of attacked state is no less than 2, i.e., $q \geq 2$. Moreover, the false positive rates are almost 0 in both noiseless and noisy 6-bus power systems. In the 57-bus system, the true positive rate is more than 90% when $q \geq 5$. Moreover, the false positive rates are near to 0 in both noiseless and noisy 57-bus power systems. That is, measurement noises can slightly reduce the true positive rates in detecting FDI attacks, and such deviation decreases with the increase of the number of attacked state. Moreover, such measurement noises have little effect on false positive rates in detecting FDI attacks.

To verify the effect of measurement noise on attack identification, we give the identification probabilities and the estimation deviation in (23). Specifically, in noise system, we calculate the average estimation deviation in cases, where attack vector $\mathbf{a}$ is exactly identified in noiseless cases. The attack identification probabilities and estimation deviations in the 6-bus and 57-bus power systems are given in Fig. 5.

As shown in Fig. 5(a), the probability of identifying FDI attacks in noisy 6-bus system is smaller than that in noiseless 6-bus system, because of the existence of measurement noises. The deviation between identification probabilities in noiseless and noisy cases decreases when the number of attacked state increases. Corresponding to the identification probability, the estimation deviation in noisy 6-bus system is larger than that in noiseless 6-bus system. The probability of identifying FDI attacks in noiseless 57-bus system is quite small, because the maximal rank of the composite matirx is much smaller than $2 \cdot (n-1)$, i.e., $r(\mathbf{M}) = 80 < 112$. Effected by the measurement noise, the identification probability in noisy 57-bus system is almost 0. Corresponding to the identification probabilities, the estimation deviation is much higher than the preset threashold. That is, in full column rank cases, such as the 6-bus power systems, measurement noises slightly reduce the porbabilities of identifying FDI attacks, and the effect of measurement noise decreases with the increase of the number of attacked state. However, in non-full column rank case, such as the 57-bus power systems, measurement noises can significantly reduce the identification probabilities, and attack vectors can hardly be identified in such cases.

To verify the effect on the operational cost in reactance perturbation, we compare the power losses on transmission lines in reactance perturbation with that of the normal case, where the transmission line's reactance is not changed by D-FACTS devices. For the 6-bus system, the power losses on transmission lines are 6.91 MW (total load is 210 MW) when the transmission line's reactance is not changed by D-FACTS devices, while the power losses are 6.61 MW by changing the reactance of line 1–2 (from 0.2 p.u. to 0.22 p.u.), line 1–4 (from 0.2 p.u. to 0.18 p.u.), line 2–3 (from 0.25 p.u. to 0.275 p.u.), line 2–5 (from 0.3 p.u. to 0.27 p.u.), line 2–6 (from 0.2 p.u. to 0.18 p.u.). Similarly, the power losses on transmission lines in the 57-bus system are 16.51 MW (total load is 1250.8 MW) when the transmission line's reactance is not changed by D-FACTS devices, while the power losses are 16.42 MW by changing the reactance of line 1–2, 1–15, 1–16, 3–4, 4–5, 4–6, 4–18, 6–7, 8–9, 9–10, 9–11, 9–12, 9–13, 11–41, 13–14, 13–15, 22–23, 24–25, 36–37, 37–38, 38–44, 41–42, 48–49, and 49–50. Obviously, compared with the case that transmission line's reactance is not changed by D-FACTS devices, the power losses in the 6-bus and 57-bus system decrease slightly for secure reactance perturbation. That is, secure reactance perturbation can not only enhance the detection and identification of FDI attacks, but also reduce the power losses on transmission lines, i.e., reduce operational cost, by optimizing the power flow on transmssion lines.

In the proposed secure reactance perturbation strategy, we make decisions on transmission line's reactance one by one, where the decision on the current transmission line's reactance is related to the other lines' reactance. Even though, solutions to the secure reactance perturbation algorithm are not globally optimal, we assert that the results can enhance the detection and identification of FDI attacks without greatly increasing the power losses on transmission lines. Measurement noises have little effect on detection probabilities, but they introduce large estimation deviations in attack identification when the composite matrix is not full column rank. Future work will study new strategies to enhance the identification of FDI attacks in non-full column rank system with measurement noises.

VI. Conclusion

In this paper, we analyze the conditions for detecting and identifying FDI attacks in the presence of secure reactance perturbation. We further design an algorithm to jointly optimize the probability of detecting and identifying FDI attacks and the operational cost associated with reactance perturbation. We demonstrate that FDI attacks can be detected with high likehood in both noiseless and noise systems, and almost all the possibel FDI attacks can be detected when the composite matrix is full column rank. Moreover, FDI attacks can also be identified with a high probablities in noiseless and noisy cases when the system is full column rank. We conclude that our proposed algorithm can enhance the detection and identification of FDI attacks without greatly increasing the operational cost of power systems.

References

[1] T. Morris *et al.*, "Engineering future cyber-physical energy systems: Challenges, research needs, and roadmap," in *Proc. 41st North Amer. Power Symp.*, Oct. 2009, pp. 1–6.

[2] D. Hadzilsmanovic, "The process matters: Cyber security in industrial control systems," Ph.D. dissertation, Centre for Telematics and Inf. Technol. (CTIT), Univ. Twente, Enschede, The Netherlands, 2014.

[3] C. Liu, J. Wu, C. Long, and Y. Wang, "Dynamic state recovery for cyber-physical systems under switching location attacks," *IEEE Trans. Control Netw. Syst.*, vol. 4, no. 1, pp. 14–22, Mar. 2017.

[4] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," in *Proc. ACM Conf. Comput. Commun. Security*, Chicago, IL, USA, Nov. 2009, pp. 21–32.

[5] M. Rahman and H. Mohsenian-Rad, "False data injection attacks with incomplete information against smart power grids," in *Proc. Global Commun. Conf.*, 2012, pp. 3153–3158.

[6] M. Esmalifalak, H. Nguyen, R. Zheng, and Z. Han, "Stealth false data injection using independent component analysis in smart grid," in *Proc. IEEE Int. Conf. Smart Grid Commun.*, Oct. 2011, pp. 244–248.

[7] J. Kim, L. Tong, and R. J. Thomas, "Subspace methods for data attack on state estimation: A data driven approach," *IEEE Trans. Signal Process.*, vol. 63, no. 5, pp. 1102–1114, Mar. 2015.

[8] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Malicious data attacks on the smart grid," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 645–658, Dec. 2011.

[9] R. B. Bobba, K. M. Rogers, and Q. Wang, "Detecting false data injection attacks on dc state estimation," in *Proc. 1st Workshop Secure Control Syst.*, Stockholm, Sweden, Apr. 2010, pp. 1–9.

[10] M. A. Rahman, E. Al-Shaer, and R. B. Bobba, "Moving target defense for hardening the security of the power system state estimation," in *Proc. 1st ACM Workshop Moving Target Defense*, Scottsdale, AZ, USA, 2014, pp. 59–68.

[11] J. Tian, R. Tan, X. Guan, and T. Liu, "Hidden moving target defense in smart grids," in *Proc. 2nd Workshop Cyber-Phys. Security Resilience Smart Grids*, Pittsburgh, PA, USA, Apr. 2017, pp. 21–26.

[12] J. Tian, R. Tan, X. Guan, and T. Liu, "Enhanced hidden moving target defense in smart grids," *IEEE Trans. Smart Grid*, Jan. 2018, doi: 10.1109/TSG.2018.2791512.

[13] K. L. Morrow, E. Heine, K. M. Rogers, R. B. Bobba, and T. J. Overbye, "Topology perturbation for detecting malicious data injection," in *Proc. 45th Hawaii Int. Conf. Syst. Sci.*, 2012, pp. 2104–2113.

[14] K. R. Davis, K. L. Morrow, R. Bobba, and E. Heine, "Power flow cyber attacks and perturbation based defense," in *Proc. 3rd Int. Conf. Smart Grid Commun.*, Nov. 2012, pp. 342–347.

[15] C. Liu *et al.*, "Reactance perturbation for enhancing detection of FDI attacks in power system state estimation," in *Proc. 5th IEEE Global Conf. Signal Inf. Process.*, Montreal, QC, Canada, 2017, pp. 523–527.

[16] G. Hug and J. A. Giampapa, "Vulnerability assessment of ac state estimation with respect to false data injection cyber-attacks," *IEEE Trans. Smart Grid*, vol. 3, no. 3, pp. 1362–1370, Sep. 2012.

[17] Y. Yuan, Z. Li, and K. Ren, "Modeling load redistribution attacks in power systems," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 659–666, Dec. 2011.

[18] J. Liang, L. Sankar, and O. Kosut, "Vulnerability analysis and consequences of false data injection attack on power system state estimation," *IEEE Trans. Power Syst.*, vol. 31, no. 5, pp. 3864–3872, Sep. 2016.

[19] A. Abur and A. G. Exposito, "Weighted least squares state estimation" in, *Power System State Estimation: Theory and Implementation*. New York, NY, USA: Marcel Dekker, 2004.

[20] Y. Mo and B. Sinopoli, "Secure control against replay attack," in *Proc. 47th Annu. Allerton Conf. Commun. Control, Comput.*, Monticello, IL, USA, 2009, pp. 911–918.

[21] S. Sridhar and M. Govindarasu, "Model-based attack detection and mitigation for automatic generation control," *IEEE Trans. Smart Grid*, vol. 5, no. 2, pp. 580–591, Mar. 2014.

[22] D. Divan and H. Hohal, "Distributed FACTS—A new concept for realizing grid power flow control," in *Proc. 36th IEEE Power Electron. Spec. Conf.*, Recife, Brazil, 2005, pp. 8–14.

[23] D. Divan *et al.*, "A distributed static series compensator system for realizing active power flow control on existing power lines," *IEEE Trans. Power Del.*, vol. 22, no. 1, pp. 642–649, Jan. 2007.

[24] K. M. Rogers and T. J. Overbye, "Some applications of distributed flexible ac transmission system (D-FACTS) devices in power systems," in *Proc. 40th North Amer. Power Symp.*, Calgary, AB, Canada, 2008, pp. 1–8.

[25] H. L. Trentelman, A. A. Stoorvogel, and M. Hautus, "Systems with inputs, and outputs," in, *Control Theory for Linear Systems*. New York, NY, USA: Springer, 2001.

[26] R. D. Zimmerman, "AC power flow, generalized OPF costs and their derviatives using complex matrix notation," MATPOWER Tech. Note 2, Mar. 2011. [Online]. Available: http://www.pserc.cornell.edu/matpower/TN2-OPF-Derivatives.pdf

[27] F. Pasqualetti, F. Dorfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," *IEEE Trans. Autom. Control*, vol. 58, no. 11, pp. 2715–2729, Nov. 2013.

[28] J. F. Geelen, "Maximum rank matrix completion," *Linear Algebra and its Applications*. Amsterdam, The Netherlands: Elsevier, 1999, pp. 211–217.

[29] K. Sou, H. Sandberg, and K. H. Johansson, "Electric power network security analysis via minimum cut relaxation," in *Proc. 50th IEEE Conf. Decision Control Eur. Control Conf.*, Orlando, FL, USA, Dec. 2011, pp. 4054–4058.

[30] V. S. Mai, D. Maity, B. Ramasubramanian, and M. C. Rotkowitz, "Convex methods for rank-constrainted optimization problems," in *Proc. Control Appl.*, 2015, pp. 123–130.

[31] A. J. Wood and B. F. Wollenberg, "Transmission system effects," in *Power Generation Operation and Control*, 2nd ed. New York, NY, USA: Wiley, 1996, ch. 4, pp. 91–130.

[32] *Power System Test Case Archive*, Univ. Washington Elect. Eng., Seattle, WA, USA. [Online]. Available: https://www2.ee.washington.edu/research/pstca/pf57/pg_tca57bus.htm, Accessed on: Jun. 18, 2018.

[33] R. D. Zimmerman, C. E. Murillo-Sanchez, and R. J. Thomas, "Matpower: Steady-state operations, planning and analysis tools for power systems research and education," *IEEE Trans. Power Syst.*, vol. 26, no. 1, pp. 12–19, Feb. 2011.

[34] A. J. Wood, B. F. Wollenberg, and G. B. Sheble, "Introduction to state estimation in power systems," in *Power Generation, Operation, and Control*. Hoboken, NJ, USA: Wiley, 2014, pp. 403–467.

Chensheng Liu (S'12) received the B.S. degree in control science and engineering from Shandong University, Jinan, China, in 2012. He is currently working toward the Ph.D. degree with the School of Electronic Information and Electrical Engineering, Shanghai Jiao Tong University, Shanghai, China. He was an international visiting graduate student with the Department of Electrical and Computer Engineering, University of Toronto, Toronto, ON, Canada, from August 2016 to August 2017. His current research interests include security of smart grid, electric vehicle navigation, and voltage control in smart grid.

Jing Wu (M'08) received the B.S. degree from Nanchang University, Nanchang, China, in 2000, the M.S. degree from Yanshan University, Qinhuangdao, China, in 2002, and the Ph.D. degree from the University of Alberta, Edmonton, AB, Canada, in 2008, all in electrical engineering. Since 2011, she has been with Shanghai Jiao Tong University, Shanghai, China, and is currently an Associate Professor. She is a Registered Professional Engineer in Alberta, Canada. Her current research interests include robust model predictive control, security control, and stability analysis and estimations for cyber-physical systems.

Chengnian Long (M'07) received the B.S., M.S., and Ph.D. degrees from Yanshan University, Qinhuangdao, China, in 1999, 2001, and 2004, respectively, all in control theory and engineering. He was a Research Associate with the Department of Computer Science and Engineering, Hong Kong University of Science and Technology, Hong Kong, and a Killam Post-Doctoral Fellow with the University of Alberta, Edmonton, AB, Canada. He has been with Shanghai Jiao Tong University, Shanghai, China, since 2009, and has been a Full Professor since 2011. His current research interests include cyber-physical systems security, mobile internet of things, and smart wireless systems.

Deepa Kundur (S'91–M'99–SM'03–F'15) received the B.A.Sc., M.A.Sc., and Ph.D. degrees all in electrical and computer engineering from the University of Toronto, Toronto, ON, Canada, in 1993, 1995, and 1999, respectively.

She is a Professor with The Edward S. Rogers Sr. Department of Electrical and Computer Engineering, University of Toronto, and currently is the Chair of the Division of Engineering Science, University of Toronto. From January 2003 to December 2012, she was a Faculty Member with the Department of Electrical and Computer Engineering, Texas A&M University, College Station, TX, USA, and from September 1999 to December 2002, she was a Faculty Member with the Department of Electrical and Computer Engineering, the University of Toronto. Her research interests lie at the interface of cyber security, signal processing, and complex dynamical networks.

Dr. Kundur has participated on several editorial boards and is currently on the Advisory Board of the *IEEE Spectrum*. She is currently a TPC Co-Chair for the IEEE SmartGridComm 2018, and also a Symposium Co-Chair for the Communications for the Smart Grid Track of ICC 2017, the General Chair for the Workshop on Communications, Computation and Control for Resilient Smart Energy Systems at ACM e-Energy 2016, the General Chair for the Workshop on Cyber-Physical Smart Grid Security and Resilience at Globecom 2016, the General Chair for the Symposium on Signal and Information Processing for Smart Grid Infrastructures at GlobalSIP 2016, the General Chair for the 2015 International Conference on Smart Grids for Smart Cities, the General Chair for the 2015 Smart Grid Resilience Workshop at the IEEE GLOBECOM 2015, and the General Chair for the IEEE GlobalSIP15 Symposium on Signal and Information Processing for Optimizing Future Energy Systems. She was a recipient of the best paper recognitions at numerous venues including the 2015 IEEE Smart Grid Communications Conference, the 2015 IEEE Electrical Power and Energy Conference, the 2012 IEEE Canadian Conference on Electrical and Computer Engineering, the 2011 Cyber Security and Information Intelligence Research Workshop, and the 2008 IEEE INFOCOM Workshop on Mission Critical Networks. She is a Fellow of the Canadian Academy of Engineering.